PHISHING AND PHARMING:
A GUIDE TO UNDERSTANDING AND MANAGING THE RISKS

JULY 2010

Acknowledgements

CPNI would like to acknowledge and thank Detica for their help in the preparation of this document. The findings presented here have also been subjected to an extensive peer review process.

A Viewpoint containing the key points of this document is also available on the CPNI public website.

Disclaimer:

Reference to any specific commercial product, process or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favouring by CPNI. The views and opinions of authors expressed within this document shall not be used for advertising or product endorsement purposes.

To the fullest extent permitted by law, CPNI accepts no liability for any loss or damage (whether direct, indirect or consequential and including, but not limited to, loss of profits or anticipated profits, loss of data, business or goodwill) incurred by any person and howsoever caused arising from or connected with any error or omission in this document or from any person acting, omitting to act or refraining from acting upon, or otherwise using, the information contained in this document or its references. You should make your own judgement as regards use of this document and seek independent professional advice on your particular circumstances.
Executive summary

This guidance provides an overview of the threat to a wide range of organisations from contemporary phishing and pharming attacks. The information presented is aimed at senior managers with responsibility for technology and information security, as well as more technical readers who will want to be updated on the issues covered in this guide.

A separate Viewpoint is also available on the CPNI website, intended as a short standalone briefing aimed at senior business leaders.

The key findings within this briefing are summarised as follows:

- Phishing and pharming attacks have become sophisticated and are being used to cause real harm to a wide range of organisations. Although a large volume of low-grade and easily defeated attacks continue to proliferate, more sophisticated attacks are succeeding against even security-aware individuals and organisations.
- Spear phishing techniques in particular are being deployed successfully and affected organisations are suffering significant business loss. In most cases, these incidents are not widely reported and this can make it difficult to assess the real scale of the problem.
- Attackers’ objectives are both to steal confidential information and to gain access to and control over sensitive systems, whether for political or financially-motivated reasons. Phishing and pharming attacks are increasingly being used as a means of delivering malicious software (malware) into target organisations, with this malware then used to achieve the attackers’ ultimate goals.
- There are a wide range of different phishing and pharming techniques which attackers may choose to employ. Alongside traditional email phishing techniques, attackers are now making use of web and mobile technologies.

Key recommendations for organisations concerned about the threat are that:

- A range of technical countermeasures should be assessed to reduce the probability that attacks will be successful.
- A range of cultural countermeasures should be adopted to increase the likelihood that employees detect attacks and are thus able to foil them.
- It must be recognised that some attacks will inevitably be successful and a range of mitigation countermeasures should be taken to limit the impact in these cases.
Understanding the threat

What are phishing and pharming?

**Phishing** is a form of electronic deception where an individual is persuaded to perform actions or divulge information by an attacker impersonating a trustworthy entity. Most Internet users have encountered phishing in the form of emails purporting to come from a bank or other business, but in fact originating from a malicious source and designed to persuade the recipient to hand over personal information such as credit card details.

Of particular concern is the emergence of **spear phishing**. A spear phishing attack targets a particular individual or group of individuals, and uses prior knowledge of the target to construct an approach that is far more likely to result in success.

**Pharming** is an attack on network infrastructure that results in a user being redirected to an illegitimate website despite the user having entered the correct web address. Such attacks succeed by exploiting weaknesses in the core technologies and processes that underpin the operation of the Internet.

Both phishing and pharming are increasingly used not only to trick targets into revealing personal information, but also as a technique for installing malicious software (malware). In the case of spear phishing this is likely to form part of a concerted infiltration and compromise operation.

How serious is the threat from phishing and pharming

Phishing and pharming attacks are being mounted by well-funded groups as a primary means of targeting organisations. In many cases the attacks are succeeding with results which are harmful to the organisation’s business interests.

The most serious cases are typically not publicly disclosed due to their sensitivity, but phishing attacks should no longer be considered as low-level crime. Gone are the days when a phishing attack would involve a user receiving a poorly crafted email that requested them to divulge login credentials for an organisation that they may or may not have had an account with. Phishing attacks are continually evolving and attackers are adding new weapons to their arsenal, resulting in attacks that are highly sophisticated, well organised, well funded and aimed at specific high-value targets with clear financial or political objectives.

While original phishing attacks were thought to deceive only the ‘naïve’, modern attacks – and spear phishing attacks in particular – are capable of deceiving the most security aware employee or customer. These attacks are succeeding and are resulting in business loss for targeted organisations.
Case study: A large organisation identified anomalous software on some machines in its network. A subsequent investigation confirmed that this software was malicious and that a large quantity of confidential information relating to a major investment programme had been stolen. The investigation concluded that spear phishing was the most likely means by which the intruder originally gained access to the network.

In a recent global survey of critical infrastructure organisations, more than half of respondents said they had been subject to stealthy infiltration of their network by a high-level adversary. We are however unable to disclose further details about this and similar case studies due to the sensitivity of the material involved to the organisations affected.

In 2008, the SANS institute ranked cyber espionage efforts by well-resourced organisations looking to extract large amounts of data (particularly using spear phishing) as one of its highest Cyber Security Menace[s]. Commercially valuable information sought includes client lists, trade secrets, expansion plans, marketing plans, personnel records, production processes, confidential financial data, customer billing information and R&D blueprints. The theft of such data could result in serious immediate and long-term impact to an organisation in terms of loss of competitiveness.

In addition, the original use of phishing and pharming as a tool for mass theft of credit card details and similar personal data continues. Phishing attacks in particular are a major component of electronic organised crime and form a significant share of all fraudulent activity. The potential profits of a successful phishing attack have resulted in increasingly skilled and motivated criminals using these attacks to make illicit gains, alongside a constant flood of lower-grade attempts.

Finally, attackers are increasingly using phishing attacks as a means of installing “back doors” into an organisation’s network. These allow the attacker to enter the network at their will: a politically motivated attacker could use this to disrupt the business of an organisation, while a financially motivated attacker might threaten to do so unless they are paid not to do so.

---

1 In the Crossfire – Critical Infrastructure in an Age of Cyber War. (Authors Stewart Baker, Shaun Waterman, George Ivanov of CSIS)


3 Corporate Espionage 201 (author: SANS Institute InfoSec Reading Room)
Sources of threat

A range of possible adversaries are using phishing and pharming techniques to achieve their malicious aims. These include:

- **Unscrupulous competitors**, particularly from nations with a weaker commitment to the rule of law or where such activities may be partially sanctioned as part of an industrial development strategy. Unscrupulous competitors will seek to steal proprietary intellectual property or commercial information that could reduce the organisation’s competitive advantage.

- **Organised criminals** who use phishing and pharming either for the direct theft of valuable personal information, or as part of a broader criminal enterprise whose objectives may include extortion and blackmail alongside theft and resale of valuable information (including as agents for unscrupulous competitors).

  Organised criminal gangs also develop and sell phishing toolkits which can be bought online for use by less technically sophisticated criminals, or by other classes of adversary. These toolkits are developed and maintained by sophisticated networks of experts with business models similar to those of legitimate software brands.

- **A number of countries** who are actively seeking UK information and material to advance their own military, technological, political and economic interests as the UK is a high priority espionage target.

- **So called “hacktivists”** who represent a serious threat. These are **politically motivated adversaries** who are seeking to embarrass and disrupt the operations of organisations or nation states to which they are opposed. Politically motivated attackers will usually target large multi-national organisations or government departments.

Phishing and pharming attacks should not be seen as isolated incidents but as part of a broader threat from well organised adversaries who will try repeatedly and through various means to achieve their malicious objectives.
The potential impact for organisations

Phishing and pharming attacks on UK organisations are succeeding and resulting in significant business impact. Although some incidents receive press coverage, in the most serious cases the potential for reputational damage from negative publicity means that there is limited or no public disclosure. Furthermore, in many cases where organisations have detected infiltration and compromise, the subsequent analysis has indicated that the original phishing attack occurred a significant time earlier, implying that many other organisations will have been successfully attacked without knowing it.

Attacks may impact organisations in different ways depending whether the attack is against the organisation’s employees or against its customers.

**Attacks on employees**

- Possible reputational damage
- Theft of valuable proprietary information
- Disclosure of sensitive information
- Loss of personal data
- Use of your infrastructure to host further attacks
- Backdoor control over your systems

**Attacks on customers**

- Direct financial loss
- Direct customer care costs
- Loss of customer confidence in use of online channel

*Figure 1: potential effects of phishing and pharming attacks*

**Attacks targeting employees**

Phishing and pharming attacks are successfully deceiving innocent employees into divulging their login credentials or unknowingly installing malicious software (malware) on their organisation’s corporate network. This is allowing attackers to gain unauthorised access to sensitive company information and systems. The implications of an attacker gaining access to a corporate network can include:

**Reputational damage**

The theft of customers’ personal information such as billing details could result in reputational damage to the affected organisation, as disclosure of such an incident would have to be made to those customers whose details were compromised. In many cases this may also be accompanied by a fine from the relevant regulatory authority.
Theft of valuable proprietary information

Attackers will frequently seek to steal commercially valuable information, which could result in a loss of competitive advantage. The information sought by attackers ranges from intellectual property such as trade secrets and engineering designs, to commercial information such as pricing or marketing plans, negotiating strategies and acquisition targets.

UK organisations have been able to confirm definite instances of theft in this manner. Other organisations have strong suspicions based on unexpected behaviour from their competitors – for example, surprisingly rapid launch of competitive products or bids won by a surprisingly small pricing margin.

Disclosure of sensitive Information

Politically motivated adversaries may seek out sensitive material to publish on the Internet or in the press as a means of embarrassing the targeted organisation (for example, the “Robin Hood Hacker” in Latvia\(^4\) who exposed the incomes of top officials after stealing millions of government tax records). Criminal adversaries may seek such material as a tool for blackmail, threatening to disclose the material if not paid a ransom.

Compromising an organisation’s infrastructure to host further attacks

Having compromised an organisation’s network, an attacker may in turn use that organisation’s corporate network to host phishing or pharming sites. If an attacker is able to compromise the organisation’s web server they may be able to create a very legitimate-seeming attack. This would be likely to result in adverse publicity.

Backdoor control over systems

Attackers are installing back doors that could be used to take control over an organisation’s key systems. This may result in the legitimate users being unable to access the systems or the systems behaving in an unwanted manner. Some criminal gangs are compromising networks and installing backdoors in order to lease them to other malicious parties. These systems could then be used for any number of malicious activities.

Attackers are also aware that the loss of productivity is a serious threat to most organisations. Attackers who have managed to install backdoors on an organisation’s networks could threaten to disrupt that organisation’s services for a period of time, unless they are paid not to. The cost of paying the attacker may appear lower than the cost of disrupted services or even than the cost of trying to detect and remove the backdoor.

However, where such payments are made, the attacker is likely to make further attempts in the expectation of further payments. Furthermore, other criminals who may learn of the payments will also be incentivised to mount similar attacks. The true cost of paying off an attacker is therefore usually much higher than the initial request.

---

**Direct cost**

Even if an organisation is able to detect an attack before the attacker achieves his or her goal, the cost of removing the attacker from the network can run to several millions of pounds. In addition to the logistical costs of identifying, gaining access to and cleaning machines which have been directly compromised, other costs can include the need to make changes to legacy software applications where embedded passwords may have been compromised by the attacker.

**Attacks targeting an organisation's customers**

**Direct financial loss and customer care costs**

If an organisation’s customer is tricked by a phishing or pharming attack, they may blame the organisation which the attacker has impersonated. Even if this blame is misplaced, it may result in the loss of business through reduced customer confidence, as well as in increased customer care costs and in many cases direct costs from making good the losses suffered.

**Loss of customer confidence in the online channel**

Depending on the severity and sophistication of the attack, it is possible that customers may be discouraged from using online services again. For instance, if a customer suffers a phishing or a pharming attack, they may lose confidence and be discouraged from interacting online with the affected organisation. This could result in higher costs as customers migrate to more expensive modes of interaction.
Modes of attack

This section outlines the various types of phishing and pharming attack. Further details are provided in an appendix (Appendix B: Modes of attack).

<table>
<thead>
<tr>
<th>Summary: types of attack</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Mass phishing</strong></td>
</tr>
<tr>
<td>- High profile</td>
</tr>
<tr>
<td>- Ranges from simple to highly sophisticated</td>
</tr>
<tr>
<td><strong>Spear phishing</strong></td>
</tr>
<tr>
<td>- Often undetected or unreported</td>
</tr>
<tr>
<td>- Targeted attack on your organisation by a determined adversary</td>
</tr>
<tr>
<td>- High impact and very difficult to defend against</td>
</tr>
<tr>
<td><strong>Pharming</strong></td>
</tr>
<tr>
<td>- Technical attack on underlying internet infrastructure</td>
</tr>
<tr>
<td>- Usually targets customers rather than employees</td>
</tr>
</tbody>
</table>

Figure 2: the types of attack

Phishing

Mass phishing attacks

Mass phishing attacks have received a large amount of media attention over the last decade. An attacker sends out deceptive emails, which appear to be from a legitimate organisation, to a significant number of email addresses. The aim is to convince some proportion of the recipients to click on an embedded link in the message that directs them to a malicious website masquerading as a legitimate one.

More recent versions of this attack do not try to persuade the user to divulge information, but rather to persuade them to perform some action. This could be visiting a website that downloads malware through a software vulnerability on the user’s machine, or opening an email attachment that contains malware. If this malware were to make it onto an organisation’s network it could have severe consequences. For instance in 2009 the Zeus trojan was reported to have affected thousands of organisations worldwide. The Zeus Trojan stole “data including 68,000 corporate login credentials…2,000 SSL (Secure Sockets Layer) certificate files and data on individuals”\(^5\)

The approach of early mass phishing attacks was very simplistic — they were produced quickly and sent to as many people as possible in the hope that a small percentage of the recipients would fall victim. While crude examples of mass phishing attacks are still frequently seen, the business of phishing has been forced to evolve as increased user awareness has threatened the profits of organised criminals.

Phishers have had time to mature the tricks they use to deceive victims into divulging confidential information or carrying out a desired action. Phishers have built up an understanding of what messages work best to deceive even the security aware users. For example, it was reported that in 2009 the FBI Director Robert Mueller confessed he had given up online banking after nearly falling victim to a phishing attack.\(^6\)

Originally simplistic attacks have rapidly evolved to become extremely sophisticated, combining clever psychology with technical approaches for designing and crafting phishing emails and websites in such a way that recipients will not be suspicious of their authenticity.

As web users have become more sceptical about the legitimacy of emails they receive, phishers have widened the variety of modes of communication they use to carry out their attacks (see appendix B which describes these modes of attack). For instance, attackers are now using SMS messages, Voice over IP and social networking to achieve their aim.

**Spear phishing attacks**

New and existing adversaries have realised that the potential of phishing goes far beyond what mass phishing attacks can offer. Adversaries have thus been investing time and effort to mature these attacks — knowing that this will result in a more successful and ultimately more fruitful attack.

Spear phishing is a highly targeted attack against a small group of individuals. It uses prior knowledge of the organisation or individual to construct an approach that is far more likely to elicit the intended response. It is a highly sophisticated attack which is frequently successful.

**Case study:** The Office of His Holiness the Dalai Lama (OHHDL) came to suspect that it was under electronic surveillance and conducted a detailed investigation.

The subsequent analysis identified that the OHHDL had been thoroughly penetrated and compromised by high-grade malware, and that the most likely method by which the initial penetration had taken place was through compromised email attachments. Carefully-written emails were sent to people working within the OHHDL, purporting to come from others in the organisation, but in fact originating from outside\(^7\).

Spear phishing attacks often target high profile individuals within organisations who typically have extensive or deep access to sensitive information. This is sometimes referred to as “Whale Phishing” or “Whaling”. The seriousness of this threat has been raised by the SANS Institute — who in 2009 identified Spear Phishing attacks designed to deliver malware as the key method of attack for its top priority cyber security risk.\(^8\)

---


\(^7\) For further information see Appendix C: Selected case studies

Spear phishing presents a more significant threat to organisations than conventional phishing attacks for a number of reasons:

- These attacks are used by sophisticated adversaries with clear malicious objectives
- They are directed against a particular organisation or group of individuals
- The probability of success is far higher because the attacker is able to socially engineer the attack more effectively
- Most users are familiar with the crude, more conventional mass phishing attacks and are able to identify them easily. They are less aware of the level of sophistication used by spear phishers.

A more detailed explanation of spear phishing attacks is provided in an appendix (Appendix B: Modes of attack).

**Modes of communication**

Both mass phishing and spear phishing attacks have made use of email, websites, SMS communication and voice calls in an attempt to deceive their victims into divulging information or performing some action.

---

**Phishing attacks and their effects**

![Diagram of phishing attacks and their effects](image)

*Figure 3: modes of communication used for phishing attacks*

Further detail on the way different modes of communication can be exploited for phishing attacks is provided in an appendix (Appendix B: Modes of attack).
Pharming

Many users are vigilant when it comes to following good security practice but almost all Internet users assume that when they type an address into a web browser they will be directed to that legitimate website. This assumption is based on the belief that core internet infrastructure is trustworthy. Unfortunately, this level of trust is misplaced.

Where a phishing attacks is an electronic form of deception that targets people, pharming is inherently a technical attack. Pharming attacks exploit vulnerabilities in core Internet technologies which were not originally designed with security in mind. To date these technologies remain extensively unchanged, despite society’s dependence on them for almost all aspects of Internet use.

The result of a successful pharming attack could be a user being redirected to a malicious website despite the user having entered the correct web address. This is because pharming is a technical attack against core Internet technologies: typically IP Routing or the Domain Name System.

Core Internet technologies

At its heart the Internet relies on two technological capabilities which make possible the exploitation of advanced wireless and fibre optic transmission systems to provide the vast range of services with which we are all familiar:

- **IP Routing** — ensures that a packet of data (a collection of ‘1s’ and ‘0s’) addressed to a numeric IP address such as 192.168.21.39 is delivered to the computing device assigned that IP address. A variety of routing technologies may be involved in achieving this, of which Border Gateway Protocol (BGP) is one.

- **Domain Name System (DNS)** — provides a lookup mechanism whereby human-friendly addresses such as “www.myorganisation.com” can be translated to the numeric IP addresses used for IP Routing. Thus (for example) a human will type a familiar web address into their browser; DNS will translate this to a numeric IP address; the browser will encode the web page request into a collection of ‘1s’ and ‘0s’ and IP Routing will then deliver the request to the web server at that IP address.

Successful attacks on DNS or IP Routing allow the attacker to manipulate to their advantage the way in which the Internet itself operates. Usually the effect is to present Internet users with a malicious website when they try to visit a legitimate one.

---

9 In practice this would often be a public IP address (rather than a private IP address as used here)
Pharming attacks on an organisation

Pharming attacks could affect an organisation in a number of ways. Firstly, pharming attacks can target customers: for example, a customer typing an organisation’s web address into their web browser could unknowingly be directed to a malicious website. This could lead to direct financial loss or theft of personal information, and could leave the customer with vastly reduced trust in the use of the Internet as a means of interacting with that organisation.

Case study: In late 2008, a successful pharming attack was mounted on CheckFree.com, a large US bill payment site. During the course of the attack, visitors to the CheckFree website were instead confronted with a blank page which attempted to install username and password-stealing malware.\textsuperscript{10}

Secondly, such an attack on an organisation’s customers could be particularly harmful if mounted by compromising that organisation’s own DNS servers (their “authoritative name servers”). In addition to the effect on directly affected customers, there could be significant reputational damage if the mode of attack became publicly known.

Finally, a pharming attack could be used to direct an organisation’s employees to a malicious server. This could lead to the potential disclosure of sensitive information or the delivery of malware, with implications for loss of confidential material and unauthorised intrusion. Such an attack could be particularly dangerous if it targeted the organisation’s own DNS or IP Routing systems rather than more generally available systems; however, it is likely that for targeted attacks spear phishing techniques will be easier and provide a better return on investment for the attacker.

\textsuperscript{10} For further details, see Appendix C: Selected case studies
Countermeasures

Three classes of countermeasure can defend against the threat from phishing and pharming.

- A range of specific **technical countermeasures** can be used either to reduce the risk of phishing attacks reaching their intended target, or to reduce the risk that a phishing or pharming attack achieves its intended goal.

- A range of **cultural countermeasures** can help to improve the likelihood that employees and customers will identify phishing and pharming attacks, thus reducing the likelihood that the attacks will succeed.

Even with a thorough combination of technical and cultural countermeasures, it is likely that a determined attacker will ultimately succeed. It is important not to rely on successful prevention but to have in place measures and plans to mitigate the effects of a successful attack:

- A range of **mitigation countermeasures** recognise that in practice a number of phishing and pharming attacks are succeeding and that some will continue to succeed despite the application of the recommended technical and cultural countermeasures. These mitigation countermeasures could make the difference between an attacker being able to cause long-term and far-reaching consequences and the attacker being unable to access any sensitive data and being quickly detected.

![Figure 5: Countermeasures.](image-url)

Having adequate countermeasures in place can be expensive, time consuming and not without significant challenges. Organisations need to balance these costs against the potentially greater costs which could be incurred from reputational damage, lost business, loss of competitive advantage and from the significant efforts which remediation can entail.
Technical countermeasures

Technical countermeasures should not be expected to eliminate the risks of being successfully phished or pharmed: no matter how much time and money is invested in them, unknown vulnerabilities will more than likely still exist.

However, a wide range of technologies exist which can significantly reduce the incidence of successful attacks. The options presented below should not be viewed as exhaustive but rather as a guide to the possible technical countermeasures available.

**Blocking malicious web traffic**

A variety of techniques can be used to identify websites which are known, or suspected of being, malicious. Such techniques include:

- Reports from people who have visited these sites and concluded that they are malicious
- Analysis of the content on the websites — for example, a website known not to be owned by a bank but nonetheless imitating the content of that bank
- Analysis of the technical behaviour of the machines which are hosting the websites — for example, indicators that suggest that the machines hosting the website are part of a botnet
- Determining that the category of website is consistent with malicious use — for example, pornography sites. However there are many more seemingly benign websites that may often host malicious content, such as websites that provide song lyrics.

Technology solutions are available that can stop users from accessing such websites. If such a website is used as part of a phishing or pharming attack, then these solutions would stop many attacks from completing.

*Figure 6: Malicious website blocking*
Such techniques can never provide comprehensive protection because attackers will always seek to disguise their malicious sites to avoid being identified until it is too late. However, a significant risk reduction can be achieved by using such solutions.

**Filtering spam emails**

Mass phishing attacks are a form of spam. Anti-spam solutions are available and are very successful at blocking a substantial amount of spam before it reaches the user. Every phishing email blocked before being delivered to a user reduces the chance of a successful phishing attack.

If not already in place, deployment of anti-spam is highly recommended. Of course, such solutions will not stop 100% of spam from being delivered since advanced spammers quickly learn ways to circumvent them. Spam filters will also provide little to no protection against spear phishing.

**Detecting and removing malicious software in the network**

Where phishing or pharming attacks are used to install malware on a corporate network, efforts should be made to detect and delete it using commercially available anti-virus and anti-spyware tools. In cases of mass phishing or pharming, this malware could be installed on many different machines around the world but most anti-virus and anti-spyware software vendors are likely to identify it at a reasonably easy stage.

Once vendors have identified the malware, they will develop signatures which can be used to detect instances of the malware inside the network. Attackers release new malware all the time: it is thus critical that anti-virus and anti-spyware signatures are frequently updated.

Advanced malware can use a range of techniques to hide from anti-virus and anti-spyware software, including explicitly disabling any instances of such software. In the case of targeted attacks such as spear phishing, the attacker may use one-off customised malware. In such cases, anti-virus and anti-spyware vendors will never see the malware and depending on its sophistication it may never be detected by their tools.

Although the limitations of anti-virus and anti-spyware software should be recognised, its use is essential to defend against a large number of easily identified malware variants.

**Blocking sensitive information leaving the corporate network**

Data Loss Prevention (DLP) technologies are available that look for defined sensitive information (such as usernames) leaving an organisation’s corporate network. If the solution detects sensitive data being sent out of the network it will block it until the user confirms that the data should be sent. This provides users with an opportunity to think twice about what they are doing before it is too late, and may in some cases be able to block the transmission of sensitive information where this is initiated by an attacker rather than a legitimate user.

It is recommended that organisations evaluate the options for deploying Data Loss Prevention solutions on their corporate network.
Patching network infrastructure

Certain attacks depend for their success on exploiting vulnerabilities within an organisation’s IT infrastructure: for example, a targeted pharming attack or a phishing website designed to install malware. Software vendors are constantly discovering new vulnerabilities and issuing patches for these to eliminate the vulnerability. It is important that such patches be applied in a timely and thorough fashion. Patches apply not only to laptops, desktops and servers but also to more specialised items of infrastructure such as routers.

In the case of more advanced attacks, the attacker may exploit a vulnerability which has not yet been discovered by the vendor and therefore no patch exists. Of course, all discovered vulnerabilities were once undiscovered vulnerabilities. Assuming that vendors continue to issue patches at the current rate, it can be inferred that a large number of vulnerabilities remain in today’s systems which have not yet been discovered by the vendors. Malicious attackers however may well have already discovered some of these remaining vulnerabilities.

Hardening network infrastructure

Alongside patching known vulnerabilities, a range of measures can be used to harden infrastructure against attack. For example:

- Unused services on servers, desktops and laptops, and on other network devices, should be turned off since increased system complexity means increased vulnerability.

- Administrative privileges (which provide users with the highest level of control over their systems) should only be used when strictly necessary, as these privileges allow a user to install software which could be malicious, and allow an attacker with an initial toehold to gain greater control over a machine.

- New hardening technologies should be continually reviewed with a view to incorporating these into IT architecture where possible. Software and system vendors are constantly innovating techniques for making the attacker’s job more difficult and can provide significant benefit. One example is the use of application whitelists to supplement traditional anti-virus and anti-malware technologies.
Using SSL and TLS

Because the Internet’s underlying IP Routing and DNS technologies were not designed with security in mind, overlay technologies such as Secure Sockets Layer (SSL) were introduced to provide an additional layer of security. SSL (and its subsequent updates now known as TLS) use cryptographic techniques to prove that a website is what it claims to be. More recently, extended certificates provide further information not just about the website identity but about the organisation that controls the website.

It is already standard practice that any online customer interaction that requests sensitive information uses SSL or TLS (such interactions can be identified by a web address starting “https://...” and by a padlock symbol shown in the user’s browser). Organisations should also ensure that any Internet-mediated transactions with their trading partners are conducted using SSL or TLS, so that those engaging in the transactions can be confident about the identity of the website they are interacting with.

SSL and TLS are not foolproof: it can be complex for users to interpret information about certificates; there have been technical attacks against the technology; and valid websites using SSL or TLS can be compromised and used for malicious ends. Ultimately, SSL and TLS are a form of electronic identity, and as with all identity schemes can be subject to identity fraud. Nonetheless, SSL and TLS is an essential tool in the fight against phishing and pharming.

Cryptographic signing of digital communication

Similar to the use of SSL and TLS, cryptographic certificates can be used to prove the identity of the sender of an email. Using appropriate software, individuals or complete organisations can be issued with a certificate which they then use to digitally “sign” their communications.
In the same way that customers and employees should look for the “padlock” symbol to validate the identity of a website before sharing sensitive information, the use of digital signatures allows them to validate the identity of the person or organisation sending them an email or other communication.

If digital signatures are widely used and relied on, spear phishing attacks will become significantly harder to carry out successfully. Software and platforms to allow the deployment of cryptographic signatures within and between organisations are readily available and recommended.

![Digital Signature: Valid](image)

*Figure 9: digital signature validation*
Cultural countermeasures

Security awareness

Creating a culture of security awareness is paramount in mitigating the risk of employees being phished. Employees need to be aware that these attacks are occurring and that they have severe implications to organisations successfully attacked. Employees should know that the worst cases are typically not publicised and that they should therefore remain vigilant at all times.

While phishing attacks have received considerable media coverage, organisations cannot simply assume that their employees are aware of these attacks. People generally trust others until they have a reason not to: phishers prey on this and if an organisation promotes vigilance it can substantially reduce its vulnerability to these attacks.

Employees should be made aware that attackers are highly skilled and will make use of advanced psychological and technical deception techniques. That said, there may be warning signs and they should know how to spot them. For instance if they receive a suspicious email they should consider:

- Is the style of writing consistent with the supposed sender?
- Is the request out of the ordinary? If there is an attached file, is it expected?
- What is the tone of the communication? Does it claim authority, stress urgency, or threaten negative consequences of non-compliance (for instance being locked out of your account)?

Employees should at the very least be aware of:

- The purpose of “padlock” icons in web browsers. If a website usually has a padlock and it has disappeared, or if the browser issues a warning about the validity of the website’s certificate, then employees should report this
- Malware and the dangers of opening email attachments
- The dangers of publishing too much information about themselves on the Internet, particularly on social networking sites. Employees should also be warned about publishing information about the organisation online (for example organisational structure, contact details and clients) as this will assist a spear phisher with their attack. Obviously, however, most organisations do require a substantial online presence.

In addition, organisations making extensive use of electronic channels to communicate with their customers should play their part in a combined effort to make UK citizens more security aware. Of course, this is a considerably harder objective than establishing such a policy within a single organisation.
Business processes

If employees have clear expectations of what genuine communications will look like, they will be better able to spot phishing attempts which do not comply with these expectations. Examples of such norms might include:

- **Communications will never request the disclosure of security credentials.** This is already common practice in most organisations: if the IT department requires access to someone’s machine, they should ask the user to complete the login or use a separate administrator account. Employees who understand this will easily spot that any communication which does request this is a phishing attempt.

- **All communications signed by an individual should come from that individual’s usual address.** Although this will naturally be the case for most communication, care should be taken to ensure this is the case for mass communications, often originating from senior management. These mass communications are often organised by an internal communications department or even by a third-party contractor.

  It is important that such (genuine) communications do not originate from, for example, John Smith [noreply@internalcomms.com]. Any such cases will desensitise employees to cases where this is an indicator of a phishing attempt:

- **Do not use embedded web links.** Rather than ask employees to click on web links embedded in communications, links should be placed on existing and well-known Intranet sites and communications should ask users to visit these sites where they will find the required link.

  Thus, rather than sending emails asking employees to “click here to update your laptop details”, the IT department should ask employees to “visit the IT department page on the Intranet and follow the ‘update my laptop details’ link”. Employees will then start to treat embedded links as suspicious and spot those phishing attempts that use this approach.

- **Promote the use of cryptographic signatures.** Public key cryptography allows communications to be “signed” in a way that provides a high level of confidence in the identity of the sender. Popular technologies already exist to deploy this to every user and to allow signatures to be verified between organisations.

  Establishing an expectation that genuine emails will be cryptographically signed will sensitise employees to treat as potentially suspicious any email which is not thus signed.

- **Establish policy of including content that supports confidence of veracity.** Authors of mails could be encouraged to include additional materials, such as references to relevant intranet content or other recent communications that recipients can then separately access to help confirm that the mail is genuine.
Establishing such norms will require appropriate training programmes but also a regular re-sensitisation of employees to deviations from those norms. Instances where genuine communications have been issued which fall outside the guidelines (and thus might be considered potentially suspicious) should therefore be regularly publicised. For maximum effect and to avoid stigmatising more junior employees, it may be desirable for such instances to be seen to have originated from senior managers and for those managers actually to take the lead in publicising their mistakes.

Organisations should establish a clear expectation among their employees that suspicious communications are reported and that such instances will then be acted on promptly. They should ensure that there are clear and above all simple mechanisms for a user to report incidents. Such a mechanism could be the presence of a “red button” at the top of all emails that employees can click to report an email as suspicious. If reporting incidents becomes a complex process then employees may become frustrated and apathetic about reporting them. It is also important that no stigma is attached to a false alarm.

Finally, where genuine phishing attempts are detected, organisations might give consideration to rewarding the notifier and should report details of the attempt. In addition to helping the general pursuit of malicious attackers, this will help to establish an expectation that attacks on that organisation are followed up, thus increasing the perception of risk to the attacker.

Policy

Organisation should have a clear communications policy clarifying the above countermeasures. Policies should be updated frequently, and cover such items as:

- How often to upgrade firewalls
- How often to upgrade anti-virus software
- How often to do data backups, and where they should be stored
- How to contact Security if a security problem is discovered.

The real challenge, however, is not writing security policies: it is communicating them effectively and creating an auditing strategy that ensures that employees are adhering to them. Organisations may benefit from retaining a marketing and communications specialist to assist with communicating internal policy to employees.

Customer expectations

In order for an organisation to minimise the risk of customers being phished by an attacker masquerading as them, they should communicate clear policies to their customers that explain how they will and will not communicate with them. This is already common practice: for example, many organisations tell their customers that they will not send them emails asking for their account details.

Harder than setting and communicating such policies, is ensuring that these are uniformly followed by employees when engaging with customers: in many instances (especially when resolving non-standard situations) the natural step is to contact the customer and ask them for information which would help with resolution.
Strong auditing of customer interactions is therefore required: when instances of non-compliant communication are detected, customers should be informed that an error was made in order to avoid dilution of their carefully set expectations.

**Mitigation countermeasures**

The technical and cultural countermeasures described in this document are essential and can reduce the likelihood of successful attacks. However, specific incidents of successful attacks against UK organisations show that a determined and persistent attacker targeting an organisation with a large number of employees will ultimately succeed.

Organisation should therefore pursue three additional countermeasures that seek not to prevent but to mitigate the impact of a successful attack:

- Firstly, high-impact sensitive information and systems within the organisation should be strongly segregated from high-threat Internet environments to ensure that a successful attacker only has access to a minimum amount of sensitive material
- Secondly, deployment of enhanced monitoring and detection can detect successful attackers early so that the situation can be remedied
- Thirdly, the organisation should make plans for remediation in order to reduce the time and cost of such exercises when they are required.

**Strong segregation**

Organisations should practice defence in depth, with the intention of limiting the impact which a successful attack may have. Where a phishing or pharming attack is used to install malware onto an employee's desktop or laptop machine (or mobile device), traditional enterprise IT architectures can make defence in depth difficult because these machines are considered to be “inside” the organisation’s boundary protections. A range of alternative options are, however, available.

Firstly, the most sensitive information and systems can be deployed onto physically separate ("air gapped") networks, which have no Internet connectivity and which users access through physically separate desktop or laptop devices. This provides an extremely strong level of protection against attacks mounted by phishing or pharming but can be costly to deploy and may frequently not provide the level of flexibility which is required to enable effective day-to-day business. This approach is warranted for those systems which could, in the event of compromise, lead to significant loss of life or to other catastrophic consequences.

Secondly, sensitive information and systems can be deployed into network environments whose only external interaction is through remote display or terminal server techniques. Employees accessing these systems will use their usual desktop, laptop or mobile devices but only for display purposes: all processing will take place in the sensitive network environment.

While malware on the employee’s desktop or laptop could in principle attack the remote display software in order to penetrate the sensitive network, this will present considerable challenges for an attacker and can provide a good level of protection. However, where
widespread employee access to such systems is required, significant costs can be incurred for the deployment of remote display servers and increased network bandwidth.

Finally, **virtualisation** is emerging as an effective approach to the segregation of sensitive information. Employees can be provided with two (or more) virtual machines on their desktop or laptop devices: where one virtual machine is compromised by a phishing or pharming attack, the resulting malware will not have access to the other virtual machine or to those systems which are only accessible from that other virtual machine.

Again, although in principle the malware could use vulnerabilities in the virtualisation technology to breach the boundary between these virtual machines, new hardware-assisted virtualisation technologies are emerging which present considerable difficulties to such attacks and can provide very strong protection without the cost of extensive additional hardware.

**Enhanced monitoring and detection**

Protective monitoring has traditionally been seen as a means of detecting attacks so that preventative measures can be taken. While this strategy continues to be essential, organisations should also conduct monitoring to detect the results of successful attacks.

A determined adversary will frequently use a phishing or pharming attack to install one-off malware crafted specifically for the job. Such malware does not provide tell-tale signatures, and signature-based monitoring is therefore of limited value. Rather, organisations should analyse log files and related data sources for indications of behaviours which might be considered suspicious: where such behaviours are found, more detailed investigation will be required in order to confirm whether or not the behaviour is in fact an indication of an intruder.

In addition, organisations should constantly evaluate the executables and other binaries installed on each machine in their network. Where unknown binaries are found, further investigation should be conducted to determine their nature and purpose. Sophisticated malware techniques such as rootkits and virtualising malware can however use a range of methods to hide binaries from naïve detection. In these cases, advanced forensic techniques are needed to detect the malware: behavioural analysis based on log files provides the pointer to cases where such forensic analysis is merited.

Such analysis is painstaking and can result in a high number of false positives, where behaviour initially believed to be suspicious is later found to be benign. However, organisations who do undertake this type of monitoring do find unwanted malware and in some cases are able to confirm that the attacker has successfully managed to steal proprietary information, authentication details, or other sensitive data.

**Planning for remediation**

When a successful attack is detected, it will be necessary to remedy the situation by removing the attacker from the network. Such remediation work may include:

- Detecting those machines which have been compromised by malware and either removing the malware or re-imaging the disks. In some cases, it may be too difficult to detect specific compromised machines or instances of the infecting malware and it may be necessary to re-image every machine in the network.
• Data may need to be rolled back to backup versions in order to remove instances of files which might have been compromised — otherwise employees opening those files could once again be reinfected

• Changing all passwords. A successful attacker may have managed to compromise all currently used passwords and if passwords are not changed then the attacker may be able to use these to re-enter the network. In addition to changing user passwords, it will be necessary to change passwords used by server software to authenticate to other servers: in many cases, legacy software may contain hard-coded passwords and it will prove necessary to find developers to modify that software.

Remediation projects can involve significant effort and take significant time, during which the attacker will continue to have access to the compromised organisation’s information and systems. Making plans in advance can reduce the level of effort and time required at the point when urgent remediation is called for: examples might include the central collation of all passwords currently used within the network or proactively identifying and removing any hard-coded passwords from legacy software.
Appendix A: countermeasures checklists

Checklist 1 – protection against primary attacks

This checklist details countermeasures which can protect against a primary attack by:

- Stopping phishing emails being received by the target
- Stopping the target of a phishing or pharming attack accessing a malicious website they are directed to, or following instructions presented on such a website.

<table>
<thead>
<tr>
<th></th>
<th>Mass phishing</th>
<th>Spear phishing</th>
<th>Phishing</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Technical measures</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Blocking malicious web traffic</td>
<td>✔️ ✔️ ✔️ ✔️</td>
<td>✔️ ✔️ ✔️ ✔️</td>
<td>✔️ ✔️ ✔️ ✔️</td>
</tr>
<tr>
<td>Filtering spam emails</td>
<td>✔️ ✔️ ✔️ ✔️</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Using SSL and TLS</td>
<td>✔️ ✔️ ✔️ ✔️</td>
<td>✔️ ✔️ ✔️ ✔️</td>
<td>✔️ ✔️ ✔️ ✔️</td>
</tr>
<tr>
<td>Signing digital communication</td>
<td>✔️ ✔️ ✔️ ✔️</td>
<td>✔️ ✔️ ✔️ ✔️</td>
<td></td>
</tr>
<tr>
<td><strong>Cultural measures</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security awareness</td>
<td>✔️ ✔️ ✔️ ✔️</td>
<td>✔️ ✔️ ✔️ ✔️</td>
<td>✔️ ✔️ ✔️ ✔️</td>
</tr>
<tr>
<td>Business processes</td>
<td>✔️ ✔️ ✔️ ✔️</td>
<td>✔️ ✔️ ✔️ ✔️</td>
<td>✔️ ✔️ ✔️ ✔️</td>
</tr>
<tr>
<td>Policy</td>
<td>✔️ ✔️ ✔️ ✔️</td>
<td>✔️ ✔️ ✔️ ✔️</td>
<td>✔️ ✔️ ✔️ ✔️</td>
</tr>
</tbody>
</table>

*Figure 10: checklist 1 – protection against primary attacks*
Checklist 2 – protection against malware attacks

This checklist details countermeasures which can protect against attacks that are designed to install malware into an organisation’s network, by:

- Stopping the successful installation of malware
- Detecting and removing malware
- Stopping malware from accessing sensitive information and systems.

<table>
<thead>
<tr>
<th></th>
<th>Mass phishing</th>
<th>Spear phishing</th>
<th>Pharming</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Technical measures</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Detecting malicious software</td>
<td>✔️ ✔️ ✔️ ✔️</td>
<td>✔️ ✔️ ✔️ ✔️</td>
<td>✔️ ✔️ ✔️ ✔️</td>
</tr>
<tr>
<td>Blocking information leaving network</td>
<td>✔️ ✔️ ✔️ ✔️</td>
<td>✔️ ✔️ ✔️ ✔️</td>
<td>✔️ ✔️ ✔️ ✔️</td>
</tr>
<tr>
<td>Patching infrastructure</td>
<td>✔️ ✔️ ✔️ ✔️</td>
<td>✔️ ✔️ ✔️ ✔️</td>
<td>✔️ ✔️ ✔️ ✔️</td>
</tr>
<tr>
<td>Hardening infrastructure</td>
<td>✔️ ✔️ ✔️ ✔️</td>
<td>✔️ ✔️ ✔️ ✔️</td>
<td>✔️ ✔️ ✔️ ✔️</td>
</tr>
<tr>
<td><strong>Mitigation countermeasures</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Strong segregation</td>
<td>✔️ ✔️ ✔️ ✔️</td>
<td>✔️ ✔️ ✔️ ✔️</td>
<td>✔️ ✔️ ✔️ ✔️</td>
</tr>
<tr>
<td>Enhanced monitoring and detection</td>
<td>✔️ ✔️ ✔️ ✔️</td>
<td>✔️ ✔️ ✔️ ✔️</td>
<td>✔️ ✔️ ✔️ ✔️</td>
</tr>
<tr>
<td>Planning for remediation</td>
<td>✔️ ✔️ ✔️ ✔️</td>
<td>✔️ ✔️ ✔️ ✔️</td>
<td>✔️ ✔️ ✔️ ✔️</td>
</tr>
</tbody>
</table>

*Figure 11: checklist 2 – protection against malware attacks*

Note that while segregation approaches can be extremely effective, neither they nor any other approach can ever provide complete security.
Appendix B: Modes of attack

Modes of attack: understanding a spear phishing attack

To understand the threat of spear phishing it is important to understand how someone may mount an attack. The figure below illustrates the spear phishing process, and some of the attacker’s key considerations at each stage.

![Spear Phishing Process Diagram](image)

**Targeting the attack**

A spear phisher will have a clear objective which typically may involve a plan for monetising the results of speculative attacks, e.g. by blackmail, sale of stolen intellectual property, competitive advantage or financial fraud.

In selecting the organisation to target, the attacker will typically consider a range of factors, including:

- the ease of obtaining information on the organisation.
Planning the attack

A pre-requisite for a spear phishing attack is obtaining some knowledge about the organisation to be attacked. The types of information that a sophisticated attacker will seek are:

- email addresses (or other electronic contacts) and job functions of a number of employees within the organisation to help select the target group more precisely
- an example of a typical corporate email, to obtain the format of the signature block and logos
- information on the organisations with which the target organisation has business relationships and the nature of these relationships
- information on a current corporate issue, (e.g. a new pensions provider, a potential merger, the appointment of new CEO, the date of reporting results, dates of internal processes such as pay reviews, promotions, etc) to enable the subject of the email to be made immediately relevant and interesting to a recipient
- information relating to the technical environment, for example what software packages are used and what technical countermeasures are in place.

Such information can be obtained from a variety of sources including:

- corporate Internet websites
- publications and news articles
- former employees
- direct elicitation (e.g. telephoning the company)
- compromised systems at other organisations, such as partners or suppliers.

Conducting the attack

The information gathered will then be used by the attacker to construct a carefully targeted approach to a small number of individuals with the aim of tricking them into performing a desired action. The desired action could be opening an attachment containing malware, clicking on a link to a malicious website or replying to the email with requested information.
The key to the success of an attack is the level of credibility of the initial approach. It needs to look real, and to be able to deceive a user familiar with standard phishing attacks. Techniques that can improve credibility include:

- spoofing the sender’s email address so that it appears to come from someone known to the recipient (and typically senior to them).
- attaching copies of real company documents.
- ensuring that the tone and format of the email is consistent with the purported sender.
- the inclusion of previous genuine emails.
- including subject matter that shows that the email comes from someone aware of current corporate issues relevant to the recipient.

**Modes of attack: phishing techniques**

Phishers will use various methods of technical deception to give the overall communication the appearance that it is legitimate. These techniques will be utilised for both mass and spear phishing attacks. The methods of technical deception will obviously vary depending on the mode of communication used.

**Deceptive email attacks**

Traditionally this has been the most popular mode of communication for both mass phishing and spear phishing.

Email attacks are effective in getting a user to visit a website or persuading them to open email attachments, which is a particularly easy way to infect systems with malware. Phishing emails are constructed in such a way that the communication appears to be from a legitimate sender. Techniques include:

- **Forging email headers.** This will give the impression that an email was sent by a trustworthy party. Whether a phishing email will flourish or flounder can be based almost entirely on the phisher’s ability to forge email headers: users are often aware of the legitimate email address of the trustworthy party, hence any deviation they will likely cause them to become suspicious. Users may not however be aware that due to the way that email works forging email headers is a trivial process: an attacker can modify the ‘From’ address of an email so that it appears to originate from any desired address. Attackers are assisted by the prevalence of ‘how to’ guides on the internet, that show in simple steps how to forge email headers.

  A more determined attacker may compromise the email account of the trustworthy party and send the email from their mailbox.
• **Having a consistent design.** An attacker will design a deceptive email message to have an appearance which is consistent with legitimate emails from the organisation which they are impersonating. Replicating the design of a trustworthy party’s email can be as simple as cutting and pasting graphics from a legitimate email into the deceptive email.

• **The use of HTML to hide links.** If an attacker aims to persuade the victim to follow a link to a website, they will send an email coded in HTML, which allows the inclusion of clickable links to a website. Such links will often not immediately display the address to which the user will be directed, and the true destination of the link may thus be concealed.

There are a variety of ways in which a phisher can do this. For instance, a simple line of code below will display the link http://www.detica.com/ in an HTML email; however if the user clicks the link (or hovers their mouse over the hyperlink) they will see that the link actually directs them to http://pleaserobme.com/:

```html
```

Phishers can also make use of url shortening services such as www.tinyurl.com/123456. These have increased in popularity, partly because some social networking sites have character restrictions, but as a result users have now developed a habit of clicking links without understanding where they are being directed. By doing so, the user is open to clicking on a malicious link.

In a sophisticated attack this link might direct the user to a plain white website that downloads malware onto their system and then quickly forwards them on to the legitimate website so that it never became clear they were visiting the wrong site.

• **Having a consistent message:** Spear phishing emails in particular require a high level of skill when they are being designed because they aim to deceive a victim into believing the email is from someone with whom they have regular contact. If there are any discrepancies between a legitimate email and the spear phishing email the target is likely to become suspicious. The attacker will thus ensure that the subject line and email attachment are consistent in order to avoid triggering suspicion.

• **Bypassing spam filters:** For mass phishing attacks, phishers make use of methods learnt by spammers to circumvent anti-spam filters. These methods aim to pass undetected through a spam filter by appearing to be legitimate, and thus to reach the targeted address. There is a constant arms race between spammers and the developers of spam filters: although spam filters can be highly effective, they are unable to get rid of all spam due to the rate in which spammers and phishers evolve their techniques.
Web delivery

Even where the initial communication is carried out using email or some other mode of communication, many phishing attacks direct users to a malicious website. Such websites are used either to persuade the visitor to divulge sensitive information, or to install malware on the visitor’s computer. More information on malware is provided later in the appendices.

There are a variety of ways that a user could be directed to a malicious website:

- The user could be persuaded to click on a link in an email that directs them to a malicious website.
- The attacker could exploit the popularity of blogs and forums to place links in comments that direct victims to malicious websites imitating genuine sites. The victim might then enter security credentials in the belief that they are accessing the real website, having followed a “helpful” link.

If an attacker hopes to convince a victim that a malicious website is in fact legitimate, they usually craft the malicious website so that it is consistent with the appearance of the target organisation’s website. An attacker can do this by:

- Making use of open source software available on the internet to copy the design and content of a website to their local machine: this can then be uploaded onto a malicious website. This malicious website will be almost indistinguishable from the legitimate website, except that its website address and SSL certificate (assuming that the target website has a SSL certificate) will not be consistent with the authentic websites.
- Registering a similar domain name. If an attacker wants to target a legitimate website named (for example) www.dontphishus.com then they could try and register an address such as www.dontph1ishus.com or www.dontphishuscom.org in the expectation that an inattentive user might not notice the discrepancy.

A website with a similar name and exact appearance of the legitimate one, which exploits users who make ‘typos’ when entering an address in the web browser could also be registered by an attacker. If a user makes a “typo” and is thus directed to the domain registered by the attacker, they may not realise that they are on a deceptive website.

- Host name obfuscation: Trying to disguise a web address (in a web browser address bar) by encoding it in a format the user will not recognise (for example hexadecimal) has long been a trick of phishers. For example, the web site www.example.com can also be encoded as www.%65%78%61%6D%70%6C%65.com. While these attacks are increasingly prevented by modern browsers that forbid such links, they can still occur if a browser has vulnerability or if the browser displays an error message (which users often ignore) as opposed to blocking it.

- Exploiting a legitimate web server: Phishers are increasingly attacking legitimate organisations’ web servers in order to host their attack on the legitimate website. A legitimate organisation may not be willing to take their website down with the result that the phishing site could remain available until administrators are able to remove it from their web server.
SSL certificates\textsuperscript{11} are designed to prove that a website is what it claims to be: in theory this should provide the user with a sense of assurance of the legitimacy of the website they visit. However, although many people are aware of the “padlock” symbol not many users understand certificates and subsequently do not check them to ensure that they are valid for the specific website they are on — even if they are issued with a browser warning. A 2009 study by Carnegie Mellon researchers found that the majority of web users in the study ignored SSL warnings\textsuperscript{12}.

\begin{figure}[h]
    \centering
    \includegraphics[width=\textwidth]{security_alert.png}
    \caption{Example of a browser warning for an invalid certificate}
\end{figure}

Even if users understand certificates and are vigilant in checking them, they can still be deceived: if an attacker is able to compromise an SSL-protected website and inject malicious code, this will be returned over HTTPS with the valid certificate displayed. Equally, SSL certificates are vulnerable to fraud as with any form of ID scheme. An attacker may steal a valid SSL certificate or register legitimately for a certificate but under a false identity.

**Man in the Middle (MITM) attacks**

An alternative to the use of malicious websites which imitate legitimate ones is the use of Man in the Middle attacks. Man in the Middle (MITM) attacks are “a form of active eavesdropping in which the attacker makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker”\textsuperscript{13}.

\textsuperscript{11} For more information on certificates, please refer to Appendix F: Online resources


\textsuperscript{13} [online] Available at: http://en.wikipedia.org/wiki/Man-in-the-middle_attack  [accessed on: 22 March 2010]
Such attacks have been developed as a means of circumventing security mechanisms such as one time passwords (OTP). As with many phishing attacks, the victims are persuaded to click on a link embedded in an email that directs them to a malicious site. In this case however, the malicious site will simply act as a proxy, relaying their traffic to the legitimate site and allowing them to conduct their business with the legitimate site as expected.

However, when they choose to log off the legitimate site, the malicious proxy will not in fact log them off – while making it appear to the target that they have logged off. At this point, the attacker is able to use the still-open connection to gain unauthorised access to the target’s account on the legitimate server.

**Mobile technology**

As mobile internet and email devices become more commonly used, they have become a target for phishers. Furthermore, websites are often rendered differently on mobile devices (e.g. they are often smaller and have limited graphics displayed) so it can be more difficult for users to determine whether they are using a genuine site.

**Text message phishing attacks** have been used to get users to visit malicious websites using the same techniques as phishing emails.

Reports of text message phishing attacks (SMShing) date back to 2006. In such attacks the victim is sent a spoofed SMS text messages that asks them to call a telephone number, respond to the message over SMS or visit a website. This attack uses similar social engineering techniques as a other phishing attacks in order to persuade the victim to comply.

These attacks are a result of criminals finding new ways to commit old crimes: in much the same way as the growth of the internet led to phishing attacks, the growth in mobile telephony and mobile internet is leading to an increased number of attacks. With mobile phone usage now ubiquitous, a massive growth is now underway in the use of mobile devices for Internet access: for example, the iPhone/iTunes combination is the fastest growing consumer technology ecosystem in history.

The growth in mobile internet use in Japan may help predict what will happen in the UK. It is widely believed that Japan leads the UK by about five years in mobile Internet use. For example, between 2006 and 2010 there was a fundamental shift in the use of Mixi, Japan’s leading social networking site — in 2006 the overwhelming majority of updates were made from standard computing devices — by 2010 more than 70% of status updates were made by mobile phone.

At present there is no mainstream anti-text message spam solution, while there are a number of solutions that allow attackers to send out thousands of text messages from a computer. It is possible to replace the Sender ID (the mobile phone number of the sender) of a SMS message with alphanumeric text. This alphanumeric text is used legitimately by organisations when sending out marketing SMS messages to customers. Organisations will

---

14 Mobile Internet Report 2009 (Morgan Stanley)
15 RSA Oline Fraud Report December 2009 — A Monthly Intelligence Report from the RSA® Anti-Fraud Command Center
usually replace the Sender ID with their organisation’s name to let them know who the SMS is from, but phishers are using this same technique to impersonate a legitimate organisation

**Mobile phone “App” attacks** have also been seen: for example, malicious mobile phone banking applications masquerading as legitimate. In highly-controlled mobile application distribution channels such as iPhone App Store, such malicious apps are relatively hard to create and distribute, but for environments with lower levels of control the distribution of malicious (but legitimate-seeming) apps is an obvious future target for phishers.

**Telephone phishing**

New technologies are often said to provide criminals with an opportunity to commit old crimes in a new fashion (for example, crimes of deception). But one would be naïve to think that criminals had suddenly stopped using old technology as a means of perpetrating their crimes. Criminals are typically ambivalent regarding which form of technology to use: they merely seek to achieve their aim without being caught. Criminals have had time to mature their abilities when using old technologies and explore new vulnerabilities in these old technologies.

Those who commit phishing attacks recognise that “it's easier to manipulate people rather than technology”\(^{16}\). This form of deception stems from the theory that people generally trust someone until they have a reason not to. By targeting this natural trust they can convince a victim to comply with his/her wishes without raising any suspicion. Users are increasingly aware of email and web attacks due to media attention and reports such as this one. Telephone attacks can be highly effective as people are often less suspicious of someone over the phone and could potentially be bullied into divulging information.

Phishing calls occur when an attacker impersonates a legitimate organisation over the phone in order to achieve their aims. As a means of convincing a user of the authenticity of a telephone call, phishers can make use of methods of technical deception such as Caller ID spoofing. Many people are not aware that attackers can spoof the Caller ID of a phone call thus if they are called from a familiar number they may be inclined to believe it is trustworthy. However attackers often will not need to do this as users are not usually familiar with the telephone number of the organisation the phisher is impersonating.

Of course, a wide range of other traditional telephone scams also continue to be pursued.

**Traditional post**

Another new use of old technology involves attackers sending out memory stick and CDs containing malware in the post. In one such example a number of Credit Unions in the USA received letters in the post from the National Credit Union Administration warning of phishing attacks. Included with this letter were two CDs that contained interactive training material. As it turned out this pack was not sent by the National Credit Union Administration and the CDs contained malware. While this attack turned out in fact to form part of a security test, it demonstrates attacks that can occur\(^ {17}\).

\(^{16}\) How to hack people [online] Available at: http://news.bbc.co.uk/1/hi/technology/2320121.stm [Accessed on: 22 March 2010]

Modes of attack: pharming

Pharming is a technical attack against core Internet technologies, in particular the IP routing and DNS subsystems.

The IP Routing and DNS subsystems on which the Internet relies are complex and dependent on the interaction of many different systems ranging from end users’ devices (laptops, desktops, mobile phones) through specialised network equipment such as routers to numerous servers providing the various subsidiary services required to deliver DNS and IP Routing.

Each of these devices is typically owned and operated by different parties: the remarkable development of the Internet is due to common agreement among all these parties as to how the various systems in the chain should cooperate.

When a malicious attacker seeks to mount a pharming attack, they may choose to attack any one of these different links in the chain:

- Firstly, on occasion attackers discover flaws in the underlying technologies such as current implementations of DNS. Examples of such flaws include DNS cache poisoning by provision of supplementary information, and the highly-publicised flaw discovered by researcher Dan Kaminsky in 2009. 18

- Secondly, the devices used to operate these core technologies can themselves be attacked. In some cases these are standard servers, while in others they are specialised devices such as routers, but in all cases these systems contain as-yet-unknown vulnerabilities which might be discovered and exploited by an attacker.

- Thirdly, the way that humans configure these devices can lead to security vulnerabilities. A common example is that home Internet users regularly leave their broadband routers set with the default password: these devices can in many cases form a key component of that user’s DNS lookup path.

- Finally, the way that humans use the devices can also be exploited by an attacker. An example of this is the use of malicious wireless access points: a user may in good faith connect to a wireless access point advertising itself as “Free public WiFi” but if this has been set up by an attacker, the attacker will then have full control over the DNS and IP Routing facilities presented to the user.

The complexity of the environment combined with the imaginative nature of the attackers mean that a vast range of attacks are possible, almost certainly including many which are as yet unknown. We therefore illustrate here a number of potential pharming attacks, but new forms of attack are constantly being invented and this is therefore a selection rather than a comprehensive list.

Local attacks

An attacker who has access to the target’s system or to other systems within the same network environment (for example, within the same enterprise network) can mount a range of local attacks in order to expand their control within this network environment. This would be the case for example where an attacker has gained an initial foothold through a phishing attack.

- **HOSTS file modification** The simplest form of pharming attack is mounted by making changes directly to the target’s machine. Of course, if the attacker already has the ability to make changes to the user’s machine then it will usually be unnecessary to mount a pharming attack, but there can be situations where even this very simple attack is useful (for example, in cases of opportunistic physical access to a machine).

The HOSTS file on an end user’s computer is a local alternative to DNS that locally maps the IP address mapping for a domain name. Real world incidents have seen attackers overwrite this file with a malicious HOSTS file: this compromised file would map commonly used web addresses to IP addresses under the attacker’s control. This has resulted in users being directed to a malicious IP address, despite having typed in the correct web address in their browser.

For example, the image below shows that by adding a record for www.detica.com that maps this address to the IP address of http://www.example.com/ the victim would be directed to the example.com website despite the browser web address bar showing www.detica.com.

![Figure 14: simple HOSTS file modification](image)
- **DHCP attack.** DHCP is a common networking subsystem that is used by client devices (laptops or desktops) on a network to request and obtain an IP address together with other required configuration information such as the DNS server and default gateway for IP routing. The client device locates and contacts a DHCP server which responds with the requested information from its database.

Like many networking protocols, DHCP is extremely efficient but should not be considered secure. Attackers have been able to run a "rogue" DHCP server on the local network of targeted organisations, such that client devices obtain their IP addresses and configuration information from this DHCP server rather than from the genuine server\(^\text{19}\). The likely result of this is a victim being directed to a malicious DNS server when they require resolution information for a web address. This is because malicious configuration information will be assigned by the rogue DHCP server.

If an attacker installs malware on one machine through a phishing attack, they could use this compromised machine to operate a rogue DHCP server and then use pharming techniques to compromise other machines on the network. It is a "sizeable challenge"\(^\text{20}\) to locate these poisoned machines.

To quote security vendor McAfee, this attack is particularly concerning because other machines on the network “...that are not infected with the malware can still have the payload of...the rogue DNS servers delivered to them. This is achieved without exploiting any security vulnerability.”\(^\text{21}\)

---

Physical attacks

In some cases, an attacker may not have access to the target’s system or to systems on the user’s local network, but may have physical access to the target’s environs. The increasing use of wireless technologies to access the Internet provides avenues for exploiting physical proximity for pharming. One such example is the “evil twin attack.”

- **Evil twin attack**: Over the past decade the number of organisations allowing their employees to connect wirelessly using technologies such as “WiFi” has skyrocketed, alongside the almost ubiquitous use of these technologies by consumer laptops and mobile devices. Wireless access points are found in offices, in public places such as airports or even in the street, and in coffee shops and cafés all over the world.

An attacker mounting an “evil twin” attack sets up a malicious wireless access point in the physical vicinity of a trustworthy access point. The malicious access point will broadcast the same or similar identity to the target’s genuine access point, in the hope of deceiving victims into believing that it is in fact the trustworthy one.

If an unsuspecting user connects to the malicious access point they will be provided with Internet access as expected, and it is unlikely that they will notice any difference between it and the legitimate access point. However, once a victim is connected to the “evil twin” access point the attacker can either eavesdrop on their wireless communication or mount a pharming attack by diverting legitimate website requests to malicious sites.
Remote attacks

Pharming attacks can also be mounted by attackers who have no local access or physical proximity. Remote attacks range in technical complexity but allow the attacker access to a huge range of targets and provide them with a low probability of retribution.

- **Drive-by pharming**: A drive-by pharming attack targets broadband routers whose owners have not changed the default username and password. Many of these routers have web-based interfaces that allow the user to update the firmware or configure the settings of their home router.

  The aim of a drive-by pharming attack is to reconfigure the DNS server settings on a victim's router, so that it requests resolution information from a malicious DNS server. These settings can be changed by posting malicious code on web pages created by a pharmer. When a victim visits one of these web pages malicious code attempts to login to the user’s home broadband router and change the DNS server settings to ones specified by the attacker.

  This malicious DNS server would then direct the user’s browser to a malicious website when a valid one is requested. For example, a request for their bank’s website could direct them to a similar-looking site operated by the attacker; or a request for a trusted software vendor’s website could direct them to a malicious site which advises them to install new software which is in fact malware.

- **Registrar account compromise**: Allied with the technologies providing DNS capabilities is a system for controlling the allocation and ownership of domain names (mybank.com, myorganisation.co.uk, etc). Organisations known as registrars manage this system on behalf of the ultimate owners of the domains.
In many cases, organisations also rely on their registrar to operate the authoritative name server(s) which are the ultimate reference for the correct mappings between host names (www.myorganisation.com) and IP addresses. To support this, registrars usually provide a web-based management system whereby the domain owner can specify the IP addresses of their web servers and mail servers.

One particularly simple means of mounting a pharming attack is to obtain the account details that are used to log onto this web-based management system, and then to use these to log on and change the configuration to specify the IP addresses of the attacker’s malicious servers. These login details might in many cases be obtained through phishing, either directed at the administrators working for the domain owner, or directed at the employees of the registrar.

Organisations should ensure they understand and are confident about their registrars' security processes before entrusting control to them of their domain name assets.

- **DNS spoofing attack**: A technically sophisticated form of pharming attack is DNS spoofing. This form of attack relies on the fact that historically DNS servers were configured to accept additional resolution information alongside the primary resolution information requested, for example from an authoritative name server.

An attacker in this case would cause a user of a particular DNS server to visit a website under their control (www.myorganisation.com, for example). This need not be the ultimate target: the attacker might for example connect to this DNS server themselves.

The DNS server will then request the resolution information for www.myorganisation.com from the relevant source — for example, from the authoritative name server for myorganisation.com.

Since the attacker controls this, they can respond as they choose: and in the case of a DNS spoofing attack they will respond not only with the requested resolution information for www.myorganisation.com, but also with the resolution information for www.mybank.com — a domain which is not under their control.

If the DNS server accepts this, it will cache the resolution information of www.mybank.com for future use, and when a user requests resolution of this address, it will not bother to contact the authoritative name server but rather, respond with the malicious IP address provided by the attacker.

Operators of DNS servers should configure their servers not to accept such additional resolution information, in order to protect against exactly this type of attack. However, instances of misconfigured DNS servers (either through accident or through ignorance) are common and this attack illustrates the type of vulnerability which may be found in systems which were not originally designed with security in mind.
• **Border Gateway Protocol attacks.** BGP "is the core routing protocol of the Internet. It maintains a table of IP networks or 'prefixes' which designate network reachability among Autonomous Systems". An Autonomous System (AS) is a collection of IP addresses that have been grouped together for administrative purposes – typically because they are all owned and operated by the same ISP.

When a packet of data is sent over the Internet, routers have to determine the "best" (in some sense) route to reach its destination. This decision is based on a constant BGP communication between routers and their neighbouring routers.

A key vulnerability in BGP is that routing is based on "trust": it is thus possible for a router to announce a "best" route which in fact does not exist, or which routes to the wrong destination. One (non-malicious) example is the incident in 2008 where a small Pakistani ISP accidentally announced itself as the world’s best route to YouTube: unsurprisingly, the world was unable to reach YouTube until this mistake was corrected.

---


Pharmers are able to exploit this “trust” and the fact that there is “no mechanism in place to guard against [parts of the infrastructure] that go rogue”\(^24\). These vulnerabilities can be exploited to announce the “best” route to any IP space, causing legitimate traffic to that IP space to be diverted to the pharmer. With correct manipulation of BGP, the pharmer could then proxy this traffic to the correct destination, thus mounting a MITM attack.

The attacker’s ability to mount such an attack would be dependent on the attacker first compromising a system which is trusted (by other ISPs) to announce routes. Nonetheless, “…everyone who connects to the Internet is currently exposed to various routing risks: downtime, hijacking and now even wholesale traffic interception …Very few people understand these risks, so they are not being measured or managed appropriately”\(^25\).

### Modes of attack: phishing and pharming malware

Phishing and pharming are increasingly used as a means of installing malware onto a target’s machine. This is not only because users have become more aware of attacks that aim to get them to divulge confidential information, but also because when targeting an organisation, a single successful attack on a single employee that installs malware on a corporate network can then be used to gain access to a wide range of the organisation’s sensitive and proprietary information.

### Types and effects of malware

Malware is a term used to describe various forms of malicious software, such as trojans, viruses and worms\(^26\).

Since the early 2000’s there has been an explosion in the amount of specialised malware that provides different mechanisms for gaining unauthorised access to a system. These include keyloggers, screen scrapers and back doors:

- **Keylogger\(^27\) / screen scraper.** Keyloggers are used to capture a user’s key strokes; in addition, mouse clicks are recorded by taking a screen shot when the user clicks the left mouse button. Keyloggers and screen scrapers hide in the memory of a host and will output the data captured to small files that will be sent to the phisher regularly. An attacker with access to a keylogger or screen scraper will be able to access all information inputted or viewed by a user including information supplied to or from secure and encrypted systems.

---


\(^{26}\) For more information on the types of malware please see the relevant appendix (Appendix F: Online resources)

\(^{27}\) Note that this section describes software keyloggers rather than hardware keyloggers. Further information about hardware keyloggers can be found in CPNI’s technical note ref TN0409
- **Back doors.** Malware is increasingly used by attackers to allow them to gain entry and take complete control of a system by installing a back door. This gives an attacker equal (or even greater) control over the system compared to the legitimate user. In addition to stealing user information and accessing the systems for which that user has permission, a backdoor gives the attacker a platform for mounting attacks against other machines in the same network. Since these attacks originate from inside the same network as the target, they have a high probability of success.

A sophisticated attacker will often use spear phishing as a means of installing an initial back door onto the machine of the target, and then use this backdoor to explore the inside of the target’s network, identify further targets and routes to obtain access to information and systems of interest.

- **Man in the Browser** malware. In a “Man in the Browser” attack, a Man in the Middle attack is mounted using malware on the user’s own machine. This type of malware inserts itself between the browser and the browser’s security mechanism, snooping on and potentially changing the transactions as they are formed on the browser but displaying back to the user what they expected to see. As with a network-based Man in the Middle attack (see earlier in this document), this can be used to evade security measures such as one time passwords.

Depending on their level of sophistication, attackers may use malware developed by third parties or may develop their own custom malware. A range of malware development toolkits are available online, and many programmers advertise their services for developing custom malware on a commercial basis.

Whether or not a particular instance of malware can be detected by anti-virus products depends on two factors: distribution and sophistication. Firstly, because one-off custom malware is not seen except in the single case where it is deployed, anti-virus products will not incorporate signatures to detect it. However, unsophisticated malware may have behaviours which are detected by anti-virus tools.

Conversely, mass distribution malware (and generic malware toolkits) is widely seen and in principle anti-virus vendors can develop signatures for detecting it. However, sophisticated malware may use advanced techniques for hiding from anti-virus software, including explicitly disabling common toolkits: malware developers test their malware against commonly found security software in order to check whether it successfully manages to evade it.

**Installation of malware**

Attackers have also been finding increasingly novel ways to persuade users to install malware onto their machines. Attacks in the wild have been seen to compromise hosts with malware through email attachments, unpatched vulnerabilities in client side applications, malicious downloads, zero day vulnerabilities, memory sticks and CDs.

- **Email attachments:** The easiest means of installing malware remains to persuade a user to open a malicious attachment in an email. Although users are increasingly wary of opening attachments from unknown sources, the objective of phishing is to persuade the recipient that the email is in fact from a known and trusted source: if this aim is achieved there is a good likelihood that the recipient will then open the malicious attachment.
**Malicious downloads:** Users often believe that the only way their computer can be infected with malware is through opening a malicious document. However, in many cases all that is required is for a user to visit a malicious website in order for that user’s system to be compromised. Such attacks are commonly known as “drive-by downloads”.

According to the SANS Institute, who ranked unpatched client side software as their number one cyber security risk in 2009, “Waves of targeted email attacks, often called spear phishing, are exploiting client-side vulnerabilities in commonly used programs such as Adobe PDF Reader, QuickTime, Adobe Flash and Microsoft Office. This is currently [2009] the primary initial infection vector used to compromise computers that have Internet access”\(^28\).

Unfortunately, also according to the SANS institute, large organisations can take twice as long to patch client side vulnerabilities as they take to patch operating systems\(^28\)\(^29\).

An alternative to “drive-by downloads” is to use social engineering to persuade a user to download and install malicious software. An example of this is malicious websites that request users to download and install codecs to play video and sound content or deceptive programs that appear to be anti-virus or anti-spyware programs when in practice they infect a victim’s machine with malware. According to the Anti-Phishing Working Group (APWG) statistics there was a substantial increase in the volume of these attacks in 2009\(^30\).

Finally, malware that could be downloaded from legitimate mainstream websites – for instance the “Asprox” virus was found on many NHS and local government websites\(^31\).

**Server-side vulnerabilities:** “Trustworthy” websites that have server-side vulnerabilities are increasingly being used by phishers to compromise user’s machines with malware. If an attacker exploits a web application vulnerability (for example through a SQL injection and Cross-Site Scripting attack) it could result in a trustworthy website being used to host malware that infects visitors’ systems through one of the techniques described above.

**Zero day vulnerabilities:** A zero day attack occurs when vulnerability is being exploited by attackers prior to the release of a patch to fix the vulnerability. This could be because the vulnerability has been announced before a patch is available. Zero day vulnerabilities are often exploited in Drive-by Download attacks. These are attacks where malware is installed simply by visiting a website, without any further action by the user.


- **Unknown vulnerabilities**: Vulnerabilities in the most commonly used client side applications (e.g. Adobe Flash, Microsoft Office) continue to be those most targeted by attackers\(^{32}\). Sophisticated attackers have access to teams conducting vulnerability research to identify vulnerabilities which are otherwise unknown: one such example is the previously unknown vulnerability in Microsoft’s Internet Explorer which was identified as a route for the attacks on Google and other parties in early 2010\(^{33}\).

- **Portable media**: As discussed earlier attackers could send out memory stick and CDs containing malware. By using this mode of infection the attackers will circumvent those security solutions and mechanisms that protect the perimeter of a corporate network from malware and from unauthorised access.

---


Appendix C: Selected case studies

Phishing and pharming attacks are regularly reported in the press, but such reports tend to focus on mass attacks: firstly, because these are of the most direct relevance to the largest number of readers; secondly, because in many instances when more targeted attacks are discovered, they are not publicly reported by the victim; and finally because while most mass attacks are detected, a high proportion of more targeted attacks are probably never detected.

This section provides a selection of case studies with varying levels of detail to indicate the types of more targeted attack which may be faced.

Example 1: Significant loss of proprietary information

A large organisation identified anomalous binaries on some machines in its network. A subsequent investigation confirmed that these binaries were malware and that significant confidential material relating to a major investment programme had been stolen.

The investigation concluded that spear phishing was the most likely means by which the intruder originally gained access to the network.

We are unable to disclose further details about this and similar case studies due to the sensitivity of the material involved to the organisation affected.

Example 2: Penetration of the Dalai Lama’s office

According to an academic report the Office of His Holiness the Dalai Lama (OHHDL) came to suspect that it was under electronic surveillance and conducted a detailed investigation.

The subsequent analysis identified that the OHHDL had been thoroughly penetrated and compromised by high-grade malware, and that the most likely means by which the initial penetration had taken place was through compromised email attachments.

Carefully-written emails were sent to people working within the OHHDL, purporting to come from others in the organisation, but in fact originating from outside. An example of such an email is shown on the next page.

---

34 The snooping dragon: social-malware surveillance of the Tibetan movement, University of Cambridge 2009
It is believed that at least one recipient of such an email opened the infected attachment, and that this gave the attacker their first foothold within the OHHDL organisation. This was subsequently expanded using other means to establish a comprehensive surveillance capability.

Example 3: Pharming attack against Brazilian bank

Brazilian press reported in 2009\(^\text{35}\) that a DNS cache poisoning attack (see Appendix B) was mounted against the customers of a large Brazilian bank. In this attack, the DNS cache for a leading Brazilian broadband provider was poisoned in order to divert customers to a malicious site which was designed to steal online banking authentication details alongside other personal information (for example, the user’s CPF number – similar to a UK National Insurance number).

According to the report, the broadband provider confirmed that before the poisoning incident was discovered and resolved approximately 1% of their customer base was affected by the attack.

Example 4: Phishing of senior executive (‘whaling’)

In 2008 the Chief Technology Officer of IT security company TippingPoint received an email from the US Federal Trade Commission (FTC). This email stated that a TippingPoint client was filing charges against the company for overcharging, and directed the recipient to

\(^{35}\) [online in Portuguese] available at: http://g1.globo.com/Noticias/Tecnologia/0,,MUL1088103-6174,00.html [accessed on: 22 March 2010]
download a Microsoft Word file detailing the complaint, and to complete and return the form included in the file.

Subsequent analysis revealed that the link contained in the email was not in fact to the FTC website (as it appeared), and that the Microsoft Word file was crafted to install a data-stealing trojan.

**Example 5: Fake subpoenas**

The New York Times has reported an incident from 2008 in which a number of senior executives in companies across the US received by email what appeared to be an official subpoena from the United States District Court in San Diego. Each message included the executive’s name, company and phone number, and commanded the recipient to appear before a grand jury in a civil case.

An example of one such email is shown below.

![Example email](image)

Each email contained a link where recipients could supposedly view a complete copy of the subpoena. However, anyone trying to view this in fact downloaded and installed malware which incorporated both a keylogger and a Trojan providing complete control over the recipient’s machine to a malicious remote user.

---

Example 6: Regular discovery of custom trojans

A large global technology company conducts regular and systematic analysis of large volumes of log files collected from devices within its global network.

The security team from this company has reported that this analysis typically reveals in any given week 1 or 2 items of malware which have never before been seen by the major anti-virus vendors. The team believes that these are often custom trojans designed specifically to infiltrate their organisation and steal intellectual property.

It is believed that a high percentage of these are delivered into the company’s network through successful phishing attacks.

Example 7: Highly targeted spear phishing

An executive working for a large organisation received an email from a contact in another company with whom he was currently corresponding in relation to a business matter. The email contained an attached spreadsheet relating to that matter, and the recipient consequently opened the attachment.

It subsequently became clear that the email had in fact been spoofed by an attacker who had gained knowledge of the discussions, and the spreadsheet had been crafted to deliver malware into the recipient’s organisation.

Example 8: Pharming attack on bill payment site

In late 2008, a successful pharming attack was mounted on CheckFree.com, a large US bill payment site. During the course of the attack, visitors to the CheckFree website were instead confronted with a blank page which attempted to install username and password-stealing malware.

The attack was mounted by stealing the authentication details for CheckFree.com’s account with their domain registrar — the company which managed their DNS records on their behalf. Using these details, the attacker logged into the account with the registrar and changed the DNS records to point to the malicious server.

There has been no confirmation as to how the authentication details were originally stolen, but it is notable that around the same period there were increased reports of phishing attacks against domain registrars.

---


38 ICANN Security and Stability Advisory Committee (SSAC) — SAC 028 SSAC Advisory on Registrar Impersonation Phishing Attacks (2008a)
Appendix D: Examples of legitimate but undesirable communications

Example 1: staff routinely use their personal email accounts to send business-related emails to colleagues and customers.

Communication amongst employees and to customers should be consistent. If users are unsure of the email address or phone number they will be contacted from then they are unlikely to be suspicious of emails originating from addresses they do not recognise.

Example 2: An organisation sends its customers their monthly statements via email. These are sent as an attachment, with the body of the email addressing the recipient as “Dear customer”

Emails should always use the recipient’s full name. This will cause a user to become suspicious if they receive a generic phishing email. Customers should not be sent attachments unless they have been requested on a one off basis and are expected.
Example 3: Members of staff are contacted by a manager asking them to visit an external website to fill in a survey. However the email is sent from the email address of a consultancy company that the manager has retained to run this survey.

External agencies should not contact employees from external email address requesting them to click links that direct them to external websites.

Example 4: The IT helpdesk of an organisation routinely asks employees to send personal details via email.

Customers or employees should never be sent emails requesting personal details.

Example 5: Employees are sent emails encoded in HTML that include links to different parts of the organisation’s website.

It is good practice to always get users to visit the website directly. Links should never be embedded in an email, as this will avoid users ever falling foul of phishing attacks.
## Appendix E: Glossary

<table>
<thead>
<tr>
<th><strong>Air-Gapped Network</strong></th>
<th>A network unable to communicate with other networks (such as the Internet) and which users access through physically separate desktop or laptop devices</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ASLR</strong></td>
<td>Address Space Layout Randomisation (see Online resources)</td>
</tr>
<tr>
<td><strong>Anti-Virus</strong></td>
<td>Solutions that detect and delete malware on a host or network</td>
</tr>
<tr>
<td><strong>Anti-Spyware</strong></td>
<td>Solutions that detect and delete spyware on a host or network</td>
</tr>
<tr>
<td><strong>Backdoor</strong></td>
<td>Malware that gives an attacker equal (or even greater) control over the system compared to the legitimate user</td>
</tr>
<tr>
<td><strong>BGP</strong></td>
<td>Border Gateway Protocol — a routing protocol used by Internet Service Providers to maintain the core functions of the Internet</td>
</tr>
<tr>
<td><strong>DLP</strong></td>
<td>Data Loss Prevention – technologies designed to reduce the level of confidential information transmitted out of an enterprise network</td>
</tr>
<tr>
<td><strong>DHCP</strong></td>
<td>Dynamic Host Configuration Protocol — a commonly utilised networking subsystem that is used by client devices (laptops or desktops) on a network to request and obtain an IP address together with other required configuration information</td>
</tr>
<tr>
<td><strong>DNS</strong></td>
<td>Domain Name Service — provides a lookup mechanism whereby human-friendly addresses can be translated to the numeric IP addresses used for IP Routing</td>
</tr>
<tr>
<td><strong>Drive-by Downloads</strong></td>
<td>An attack where malware is installed simply by visiting a website, without any further action by the user</td>
</tr>
<tr>
<td><strong>Drive-by Pharming</strong></td>
<td>An attack that reconfigures the DNS server settings on a victim’s router, so that it requests resolution information from a malicious DNS server.</td>
</tr>
<tr>
<td><strong>Extranet</strong></td>
<td>A private network that allows for external access over the internet</td>
</tr>
<tr>
<td><strong>Evil Twin</strong></td>
<td>An attack where a malicious wireless access point is set up in the physical vicinity of a trustworthy access point. The malicious access point will broadcast the same or similar identity to the target’s genuine access point, in the hope of deceiving victims into believing that it is in fact the trustworthy one</td>
</tr>
<tr>
<td>Term</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Firewall</strong></td>
<td>A security solution that blocks unauthorised access to a network</td>
</tr>
<tr>
<td><strong>Host Name Obfuscation</strong></td>
<td>A method of obscuring a domain name in the browser address bar</td>
</tr>
<tr>
<td><strong>HOSTS File</strong></td>
<td>A local alternative to DNS that locally maps the IP address mapping for a domain name</td>
</tr>
<tr>
<td><strong>HTML</strong></td>
<td>Hypertext Markup Language</td>
</tr>
<tr>
<td><strong>HTTP</strong></td>
<td>Hypertext Transfer Protocol:</td>
</tr>
<tr>
<td><strong>IP</strong></td>
<td>Internet Protocol</td>
</tr>
<tr>
<td><strong>IP Address</strong></td>
<td>A numeric address that is assigned to all computers and network devices on the internet</td>
</tr>
<tr>
<td><strong>IP Routing</strong></td>
<td>Ensures that a packet of data addressed to a numeric IP address is delivered to the computing device assigned that IP address.</td>
</tr>
<tr>
<td><strong>Malware</strong></td>
<td>Malicious Software</td>
</tr>
<tr>
<td><strong>MITB</strong></td>
<td>Man-in-the-Browser — This type of malware inserts itself between the browser and the browser’s security mechanism, snooping on and potentially changing the transactions as they are formed on the browser but displaying back to the user what they expected to see</td>
</tr>
<tr>
<td><strong>MITM</strong></td>
<td>Man-in-the-Middle — an attack where an attacker acts as an active intermediary between two trustworthy victims</td>
</tr>
<tr>
<td><strong>Patch</strong></td>
<td>A ‘fix’ for a software vulnerability</td>
</tr>
<tr>
<td><strong>Phishing</strong></td>
<td>An electronic form of deception where an individual is deceived into performing actions or divulging information by an attacker impersonating a trustworthy entity</td>
</tr>
<tr>
<td><strong>Pharming</strong></td>
<td>An attack on network infrastructure that results in a user being redirected to an illegitimate website despite the user having entered the correct web address</td>
</tr>
<tr>
<td><strong>OTP</strong></td>
<td>One Time Password – a password that is only valid once</td>
</tr>
<tr>
<td><strong>Registrars</strong></td>
<td>Those who manage domain name information and systems on behalf of the ultimate owners of those domains</td>
</tr>
<tr>
<td><strong>Remote Display</strong></td>
<td>Employees accessing these systems will use their usual desktop, laptop or mobile devices but only for display purposes: all processing will take place on a separate system</td>
</tr>
<tr>
<td><strong>Rootkit</strong></td>
<td>A form of malware (see Online resources)</td>
</tr>
<tr>
<td><strong>SMShing</strong></td>
<td>SMS (text) message phishing</td>
</tr>
<tr>
<td><strong>Spear Phishing</strong></td>
<td>A highly targeted phishing attack against a small group of individuals</td>
</tr>
<tr>
<td><strong>SSL</strong></td>
<td>Secure Sockets Layer – a technology which uses cryptographic techniques to prove that a website is what it claims to be</td>
</tr>
<tr>
<td><strong>TLS</strong></td>
<td>Transport Layer Security – the successor technology to SSL</td>
</tr>
<tr>
<td><strong>Trojan</strong></td>
<td>A form of malware (see Online resources)</td>
</tr>
<tr>
<td><strong>Virtualisation</strong></td>
<td>A method of running multiple computer environments (virtual machines) on the same physical machine</td>
</tr>
<tr>
<td><strong>Virus</strong></td>
<td>A form of malware (see Online resources)</td>
</tr>
<tr>
<td><strong>Vishing</strong></td>
<td>Voice Phishing</td>
</tr>
<tr>
<td><strong>Voice Over IP</strong></td>
<td>Telephone calls made using Internet technologies</td>
</tr>
<tr>
<td><strong>VPN</strong></td>
<td>Virtual Private Network – a network that allows for users to securely access a network remotely</td>
</tr>
<tr>
<td><strong>Web Server</strong></td>
<td>Software or hardware that serves web page content</td>
</tr>
<tr>
<td><strong>Whitelist</strong></td>
<td>A list of trusted sources</td>
</tr>
<tr>
<td><strong>Whale Phishing</strong></td>
<td>A spear phishing attack that targets high profile individuals within organisations who typically have extensive or deep access to sensitive information</td>
</tr>
<tr>
<td><strong>Worm</strong></td>
<td>A form of malware (see Online resources)</td>
</tr>
<tr>
<td><strong>Zero Day Vulnerability</strong></td>
<td>A zero day attack occurs when vulnerability is being exploited by attackers prior to the release of a patch to fix the vulnerability</td>
</tr>
</tbody>
</table>
Appendix F: Online resources

Border Gateway Protocol
  www.bgp4.as

SSL and Digital Certificates

Domain Name Services
  http://www.internic.net/faqs/authoritative-dns.html

Malware
  http://www.kaspersky.com/threats_faq
  http://www.sophos.com/blogs/chetw/g/2010/04/03/3-types-viruses-demystified/

General Phishing information
  http://www.antiphishing.org/
  http://www.getsafeonline.org

Technical Solution Guides
  http://www.gartner.com
  http://www.forrester.com

Vulnerabilities
  http://www.kb.cert.org/vuls/

Centre for the Protection of National Infrastructure
  CPNI’s public website contains a number of relevant resource products
  http://www.cpni.gov.uk/