

Phishing & Pharming

- Do you ever receive unsolicited emails?
- Do you ever open emails without validating the source?
- Do you ever follow the links to websites from emails?
- Do you carry out banking or payment transactions online?
- Do you go directly to websites from links in your favourite sites list?



If you answered yes to any of the above questions then your business may be at risk.

Description

“Fraud cost UK online banking victims £56.1m during 2006 and 2007.”

Fraud: The Facts 2008 – APACS

Phishing involves criminals sending out ‘bait’ emails in order to see how many unsuspecting users they can ‘hook’. Phishers hijack brand names of banks, web retailers and credit card companies, send out spoof emails and use fraudulent websites to trick people into giving out personal financial data. The branded email appears credible but its aim is to steal your data and money.

Bogus emails may also contain malware scripts such as viruses and spyware that execute when you open the message.

Pharming is similar to a phishing attack in that the aim of the fraudster is to steal sensitive information. Users are directed to fake sites via bogus emails, viruses or spyware, whilst trying to access legitimate websites. Viruses can swap legitimate websites in your favourites list to scam sites so what looks like a familiar internet banking site is actually a fraudulent one.

CASE STUDY

Diving Equipment Supplier, North East England

Most people are aware of the scam emails that come in purporting to be from your bank, however, what happens if you receive an email from one of your trusted suppliers?

The above company has an international customer base. They supply diving equipment worldwide and use an e-commerce system. Any customer can enter their account details and have the product sent to them. The purchaser receives the confirmation of sale, invoice and delivery details via email to their designated email address, so receiving emails from the company did not seem out of the ordinary.

When customers received emails with their company branding on asking for clients to follow the link and update their account details due to server problems, they did not question it. Cyber criminals set up a false website mimicking the authentic one with a view to stealing customer data and money.

The business did learn of the scam but not until it was too late. A number of customers had already followed the link and divulged sensitive information before losing money from their credit cards. Not only had their clients lost money but the reputation of the company was severely damaged.

The company now regularly advises customers that they will never ask for account information via email and encourage customers to report any unusual email activity. Educating employees, colleagues and clients as to the danger of phishing and pharming scams is important. Companies should also regularly check their websites for subtle changes, indicating a scam may be in operation.

Solutions

- + Regularly check your accounts for unusual activity
- + Install anti-virus and anti-spyware and regularly run updates
- + Install a personal firewall to block incoming attacks
- + On secure websites look for the https on the address bar – the extra s indicating secure
- + Look for the padlock in the bottom corner. This indicates a security certificate. A padlock can be faked so click on it to open and ensure it is in date and reflects the correct address
- + Consider a firewall for your server to ensure that attacks are stopped before accessing the network
- + Share examples and experiences of scams with other users in the network
- + Inform clients that you will never ask for personal information via email and to report suspicious mail
- + Ensure clients, colleagues & employees are aware of scam emails and to not divulge any personal information or click on links to other sites
- + Regularly check your websites for subtle changes
- + Use Domain Name System (DNS) protection to ensure that a DNS server cannot be hacked. DNS is a system of servers located throughout the internet that handle surfing connections and email routing.

Business Type	Method of Attack	Negative Consequences	Solution	Cost
BASIC + Not linked to the internet + Administration only	+ N/A	+ N/A	+ N/A	+ N/A
ONLINE COMPUTER USER + Single machine linked to the internet + Receive email/transact online (includes laptops, smartphones, Blackberrys, PDA's)	+ Via email + Via bogus website + Via malware redirecting you to pharming site	+ Theft of sensitive data + Theft of money + Infection from viruses	+ Check your accounts + Install anti-virus and anti-spyware + Install a personal firewall + Look for the https on the address bar + Look for the padlock in the bottom corner + Install the latest web browser + Limit access to websites except for business use	+ No cost + Low cost + Low - High cost + No cost + No cost + No cost + No cost
NETWORKED + Same as above, but a collection of computers form a network (The risk increases as there are potentially more staff, increased computer business activity, therefore increased exposure to the risks)	Methods the same as above	As above	Solutions the same as the above but also: + Install a firewall for your server + Share examples and experiences of scams	+ High cost + No cost
ONLINE TRADER + Uses an e-commerce strategy to sell products to a global audience (Risk is again generally enhanced as the business and turnover is totally reliant on computer systems functioning correctly)	Methods the same as above	As above but also: + Loss of clients sensitive information + Damage to company reputation and loss of business	Solutions the same as above but also: + Inform clients of your information collection policy + Ensure clients, colleagues and employees are aware of scams + Check website for changes + Use Domain Name System (DNS)	+ No cost + No cost + No cost + Medium cost

Useful Websites

- <http://www.ktn.qinetiq-tim.net/>
- <http://www.berr.gov.uk/whatwedo/sectors/infosec>
- <http://www.bcrc-uk.org>
- <http://www.businesslink.gov.uk>
- <http://www.getsafeonline.org/>
- <http://www.sophos.com/security>
- <http://zdnet.co.uk/toolkits/securitythreats>
- <http://www.sophos.com/security/best-practice/phishing.html>
- <http://www.banksafeonline.org.uk> – safe online banking / report scams