Defending Against Phishing & Social Engineering Attacks

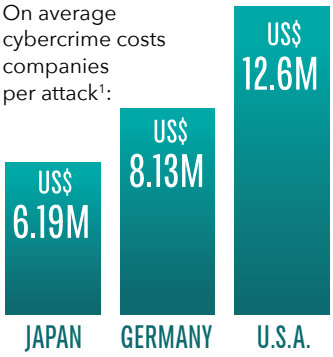
A Resource Guide from the PCI Security Standards Council

Hackers use **phishing and other social engineering** methods to target organisations with legitimate-looking emails and social media messages that **trick users into providing confidential data**, such as credit card number, social security number, account number or password. These attacks are at the heart of many of today's most serious cyberhacks and **can put your business and your customers at risk**. With a few security basics and ongoing vigilance, businesses can be aware and defend against these attacks.

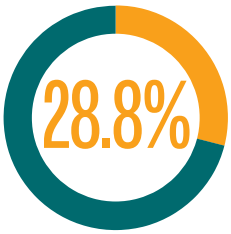
UNDERSTANDING THE RISK

THE COST = THEFT OF CUSTOMER DATA **+ DAMAGE** TO YOUR COMPANY'S REPUTATION **+ LOST REVENUE** AND FINES

On average cybercrime costs companies per attack[1]:



of annual cybercrime cost for companies is due to phishing and social engineering[1].



of phishing attacks in 2014 were intended to steal financial data from users. While carrying out their scams, cybercriminals have shifted their focus from banks to payment systems and online shopping sites[2].

The average **time it takes a company to resolve a cyberattack** caused by phishing and social engineering[1].

1: Source: 2014 Global Report on the Cost of Cybercrime 2: Source: Financial Cyberthreats in 2014

THE ATTACK

Hackers target organisations using specially crafted legitimate looking emails and social media messages that trick employees into providing confidential data that can be used for fraud.

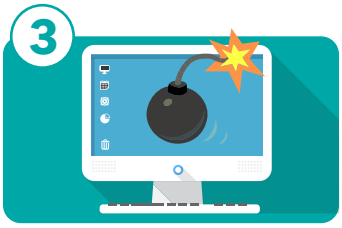
HOW HACKERS TRICK YOU

RECONNAISSANCE

- Information gathering from various online sources and social networking sites
- Business applications and software

SOCIAL ENGINEERING

- Phishing emails or messages coming from a target's social network
- Phone call from assumed known entity

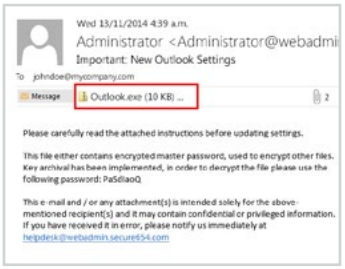


BREAK-IN

- Delivery through email
- Software vulnerabilities that can be exploited

PCI Security Standards Council

HOW HACKERS BREAK IN



PHONY EMAILS

Send emails with attachments containing malicious software that infect your computer and system, or with links to malicious sites that look like valid sites

WEBSITE AND SOFTWARE VULNERABILITIES

Browse websites where users voluntarily or involuntarily trigger vulnerabilities in Flash and Java that open them up to attack

COMPROMISED CREDENTIALS

Gain remote access to a network by using unauthorized usernames and passwords

PROTECT YOUR BUSINESS

EMAIL AWARENESS

Every day 80,000 people fall victim to a phishing scam, 156 million phishing emails are sent globally, 16 million make it through spam filters, 8 million are opened[1].

Reduce unwanted email traffic:

- Install and maintain basic security protections, including firewalls, anti-malware software and email filters.

Train employees and users on email and browser security best practices, including these key tips:

- Resist the urge to click links in a suspicious email; visit websites directly.
- Be cautious of email attachments from unknown sources. Also, many viruses can fake the return address, so even if it looks like it's from someone you know, be wary about opening any attachments.

WEBSITE AND SOFTWARE SECURITY

99.9 percent of data breaches were a result of a hacker exploiting bugs that had a fixable patch for at least a year[2].

Separate and update computers and software:

- Keep computers used for social media sites, email and general internet browsing separate from computers used for processing financial transactions.
- Use basic security tools that block malicious intruders and alert you to suspicious activity, including firewalls, anti-virus, malware and spyware detection software.
- Regularly check that web browsers and security software have the latest security patches and updates.

Train employees and users on website and browser security best practices, including these key tips:

- Only install approved applications.
- Be sure you're at the right website when downloading software or upgrades. Even when using a trusted site, double check the URL before downloading to make sure you haven't been directed to a different site.
- Recognize the signs that your computer is affected and contact IT.

PASSWORD PROTECTIONS

Password1 was the most common password used by businesses in 2014[3].

Practice good password hygiene:

- Change the passwords on computers and point-of-sale systems (including operating systems, security software, payment software, servers, modems, and routers) from the default ones the product came with to something personal to you but that is difficult to guess - such as combining upper case letters, numbers and special characters, or using a passphrase.
- Update system passwords regularly, and especially after outside contractors do hardware, software or point-of-sale system installations or upgrades.
- Educate employees and users on choosing strong passwords and changing them frequently.

Use two-factor authentication:

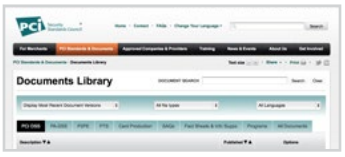
- Many of these attacks rely on getting a password one way or another. Requiring another form of ID, such as security tokens, will make it harder for hackers to falsify an account.

1: Source: Get Cyber Safe 2: Source: Verizon Data Breach Investigation Report 3: Source: Trustwave

PCI Security Standards Council

PCI RESOURCES

pdf Protect your online business against cyberattacks



www PCI Data Security Standard (PCI DSS)

- Email security awareness – Requirement 8.4
- Website and software security – Requirements 1 (firewalls), 5 (protect against malware and viruses), 6 (secure systems and applications)
- Passwords – Requirements 8.2, 8.2.1-8.2.6, 8.3, 8.5

pdf PCI Security Standards Council Best Practices for Implementing a Security Awareness Program

pdf Guide to Safe Payments

pdf It's time to change your password

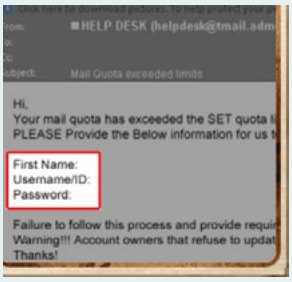
For expert comment or questions, please contact: press@pcisecuritystandards.org
For more information on PCI Standards and resources, visit: www.pcisecuritystandards.org.

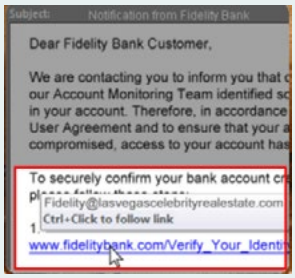
WHAT IS "PHISHING"

A form of social engineering where an attempt to acquire sensitive information (for example, passwords, usernames, payment card details) from an individual is made through e-mail, chat, or other means. The perpetrator often pretends to be someone trustworthy or known to the individual.

If it Looks Like a Phish… Signs of a Phishing Email:

- Comes from a known entity or contact
- Asks for personal information, such as employee number, credit card details, account log-in or password
- Urgent wording, grammatical errors, generic addressee
- Tells you to click on a link that takes you to a website where your confidential information is requested





PCI Security Standards Council