CREST
CENTRE FOR RESEARCH AND EVIDENCE ON SECURITY THREATS

5 MINUTE READ | PROTECTIVE SECURITY PROFESSIONALS

INTRODUCTORY GUIDE: WHY DO PEOPLE CLICK ON PHISHING LINKS?

This short guide summarises the different approaches to phishing and outlines the main reasons that people click on phishing links.

HOW DOES IT WORK

"Criminals can utilise online data to tailor phishing techniques to a person's preferences and trick them into disclosing personal information."

Phishing is the attempt to gain personal information through the use of fake emails and websites. Fraudsters typically masquerade as reputable organisations or trustworthy individuals and persuade people to disclose personal information by clicking on links or filling in forms.

Phishing is a major problem because people disclose and manage much of their personal information online (e.g. shopping, bills, bank accounts). People also provide detailed information about their interests through social media. Criminals can utilise this online data to tailor phishing techniques to a person's preferences and trick them into disclosing personal information. It is a common approach used in cyber-security attacks, with the UK Government and critical national infrastructure increasingly targeted. This document summarises the different approaches to phishing and outlines the main reasons that people click on phishing links.

TYPES OF PHISHING

There are a number of approaches used by phishers, which include email/spam, instant messaging, link manipulation (deceptive links that send users to a phishing website) and content manipulation (content on a reliable website is manipulated to divert users to a phishing website). Specific types of phishing include:

- **Spear phishing** - directed at specific individuals or companies. Attackers may gather personal information about their target to increase the probability of success.
- **Clone phishing** – phishers use the contents and receiver's address from a previously sent, legitimate email and replace the content with a phishing link and a fake reply-to address.
- **Whaling** - phishers target businesses and high profile senior executives. The content will be designed to appear more serious to appeal to the upper-management of a company.

WHY IT WORKS

Specific influence techniques are frequently used to encourage users to click on links. The following table lists the most prevalent techniques and examples of what they might look like.

INFLUENCE TECHNIQUE	EXAMPLE
Communication norms: Information that a person receives often, or is expecting to receive is unlikely to be questioned.	A typical work-related topic may go unnoticed – "Your inbox is full"
Compliance with authority: People are more likely to complete a task when instructed to do so by a high status individual or respected institution.	"Your bank manager requires you to update your details…"
Distraction: Distraction techniques limit a person's attention or cognitive resources meaning they are less likely to think about or notice the phishing attempt.	A pop-up box may be designed to divert the user to a fraudulent website when it is closed.
Encouraging emotional responses: Provoking an emotional response can cause people to take action.	"Complete this survey for a £10 reward"
Group conformity: Creating the impression that other people are doing something makes a person feel the need to comply.	"75% of members have already signed up, don't miss your chance"
Increased sophistication: Whilst many people may be aware of the risks and symptoms of phishing, new, more sophisticated techniques are being developed, making attacks more difficult to detect.	Improved spelling, grammar, layout and a "professional" appearance makes a sender appear trustworthy.
Information of interest: Generating curiosity or the perception that the information is interesting increases the likelihood that the person will want to find out more.	"Click here to arrange the delivery of your package…"
Urgency: Instilling a sense of importance and the need for a quick response.	"Your account will be deleted unless you verify your details"

ADDITIONAL FACTORS

It is likely that the success of these influence techniques will be affected by a number of contextual factors. For instance, an individual's IT skills/experience may affect their susceptibility — they may be more vulnerable to phishing attacks if they do not know what signs to look for or the range of phishing attacks that can occur. Some other factors that may affect the success of phishing attempts include: an individual's position within an organisation; their demographic/cultural background; language and personality traits. However, there is little conclusive evidence on the extent to which, and how, these factors affect the success of phishing attempts.

WHAT CAN USERS DO?

In attempting to reduce the success of phishing attacks, users can take a number of preventative measures:

- Check the sender of the email, and that the claimed link goes to where it claims.
- Refrain from clicking links or opening attachments in suspicious email messages.
- Type addresses into a browser (rather than clicking links directly), particularly when visiting a bank or financial institution.
- Check security certificates on websites before entering personal or financial information. Self-signed security certificates are one of the signs of a dubious website.
- Refrain from entering personal/financial information into pop-up windows or from forms embedded in email messages.
- Keep computer software current with regular security updates.
- Before signing up to a website, read their privacy policy to establish whether the organisation sells its mailing lists.

WHAT CAN ORGANISATIONS DO?

Organisations can help protect users by taking a number of simple steps:

- Avoid sending out phishing like emails to their users, and make clear to their customers or staff what to expect from an email from the organisation. For example organisations can inform customers and staff that they will never make requests for personal data in emails.
- Where appropriate, provide training to users in the IT-skills required to identify phishing emails and the influence techniques used.
- Provide additional security awareness to high-net-worth individuals or those with financial authority.
- Use the information from cyber-intelligence services to identify and monitor online threats e.g. Cyveillance and Mark Monitor.
- Implement multiple security controls to protect data. For example, users can be asked to supply multiple forms of authentication when attempting to access accounts (username, password, account number etc). Organisations can also request verification by using alternative communication channels (phone calls or text messages) to validate a person's identity.
- Use digital signatures to provide assurance of the origin, identity and status of a message.
- Limit the amount of personal details published about staff online.
- Use the data from any phishing emails that are received (e.g. the from and subject fields) to adjust email filters to block similar messages. Change passwords for any users that have been affected by phishing attempts

READ MORE

Atkins, B., & Huang, W. (2013). A study of social engineering in online frauds. *Open Journal of Social Sciences*, 1(03), 23.