Cybersecurity User Awareness Guidelines

What is a “phishing” or “scam” attack?

In short, it’s a process for identity theft where cybercriminals try to get users to hand over personal and sensitive information (without them knowing it). Interestingly, phishing has – in one form or another – been around for years via phone calls and physical letter scams.

Cybercriminals have typically deployed phishing attacks after a breach. This was the case with large data breaches, where criminals sent out warnings to users advising them to change their passwords (but directing them to a fake website in an attempt to harvest their details).

However, some information security pros now believe that cybercriminals view phishing attacks as a successful (and easy) way of getting into an enterprise to launch more sophisticated attacks. Humans are, after all, increasingly seen as the weakest link (insider threats are a big problem) and thus the most effective target for criminals looking to infiltrate an enterprise or SME.

1. Be Sensible

You can significantly reduce the chance of falling victim to phishing attacks by being sensible and smart while browsing online and checking your emails.
Be cautious when downloading any software from the web. A legitimate piece of software could be saddled with piggyback spyware, or even contain keyloggers or screen scrapers that could be used to steal your information. You should avoid free screensavers and other freebies. In addition, you should also be wary when opening email attachments (such as a video, graphic, or a PDF), even if they are from someone you know. Avoid anything that requests id and password information for systems that you use unless it is the system itself.
You should never click on links in an email to a website unless you are absolutely sure that it is authentic. If you have any doubt, you should open a new browser window and type the URL into the address bar.
Be wary of emails asking for confidential information – especially if it asks for personal details or banking information. Legitimate organizations, including and especially your bank, will never request sensitive information via email.

2. Watch out for shortened links

You should pay particularly close attention to shortened links, especially on social media. Cybercriminals often use these – from Bitly and other shortening services – to trick you into thinking you are clicking a legitimate link, when in fact you’re being inadvertently directed to a fake site. E.g. https://bit.ly/2p7Rdzc (This one takes you to www.itsupportworx.com)
You should always place your mouse over a web link in an email to see if you’re actually being sent to the right website – that is, “the one that appears in the email text” is the same as “the one you see when you mouse-over”.

Cybercriminals may use these 'fake' sites to steal your entered personal details or to carry out a drive-by-download attack, thus infesting your device with malware.

3. Does that email look suspicious? Read it again

Plenty of phishing emails are fairly obvious. They will be punctuated with plenty of typos, words in capitals and exclamation marks. They may also have an impersonal greeting – think of those 'Dear Customer' or 'Dear Sir/Madam' salutations – or feature implausible and generally surprising content.

Cybercriminals will often make mistakes in these emails … sometimes even intentionally to get past spam filters, improve responses and weed out the 'smart' recipients who won't fall for the con.

4. Be wary of threats and urgent deadlines

Sometimes a reputable company does need you to do something urgently. For example, in 2014, eBay asked its customers to change their passwords quickly after its data breach.

However, this is an exception to the rule; usually, threats and urgency – especially if coming from what claims to be a legitimate company – are a sign of phishing.

Some of these threats may include notices about a fine or advising you to do something to stop your account from being closed. Ignore the scare tactics and contact the company separately via a known and trusted channel.

5. Browse securely with HTTPs

You should always, where possible, use a secure website (indicated by https:// and a security "lock" icon in the browser's address bar) to browse, and especially when submitting sensitive information online, such as credit card details.

You should never use public, unsecured Wi-Fi for banking, shopping or entering personal information online (convenience should not trump safety). When in doubt, use your mobile's 3/4G or LTE connection.

As a slight aside, it should be easier to spot dodgy, unsecure websites – Google, for example, is looking to crack down on this soon by labelling sites that do not offer appropriate protection.