includem

Phishing Awareness

Email phishing (pronounced: fishing) is an extremely popular form of cybercrime because of how effective it can be. Cyber criminals have been successful using emails, text messages, direct messages on social media or even in video games to get people to respond with their personal information. The best defence is raising staff awareness and knowing what to look out for.

Unfortunately, these types of scams are on the rise and it is extremely important that staff know how to spot a phishing message.

Phishing Attack Simulation

We recently carried out our own internal test where a simulated phishing attack message was sent to all staff. This was in the form of an email which you would have received between 14th and 24th November with an apparent shared file from the Systems Administrator.

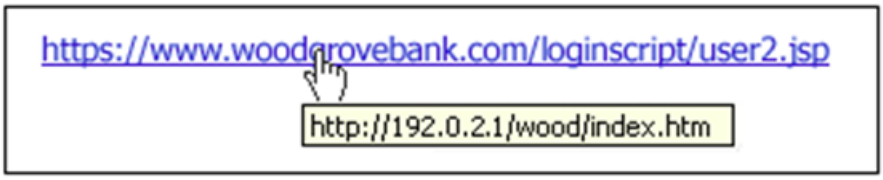
There were 165 emails sent in total; 40 members of staff did not open the email or deleted straight away; 79 members of staff opened the email; 30 members of staff clicked the link and 16 staff submitted their details when prompted.

The good news is that no harm has come this time but we urgently need to plan in next actions to ensure staff are fully aware of these types of risks and what the consequences of falling for these are which could result in major consequences for the Organisation.

Due to these alarming numbers, we will be planning and introducing increased staff awareness messages and sessions across the organisation to ensure these types of risks are eliminated and staff know what to look out for in the future.

Whilst there should are immediate red flags that you should look out for in any email i.e. the senders email address, language used in the email and the 'External' banner that's specified on all Includem emails that are sent when the sender is from outside of the Organisation, see below for some quick guidance on how to spot a Phishing message:

- Urgent call to action or threats - Be suspicious of emails that claim you must click, call, or open an attachment immediately. Often, they'll claim you have to act now to claim a reward or avoid a penalty. Creating a false sense of urgency is a common trick of phishing attacks and scams. They do that so that you won't think about it too much or consult with a trusted advisor who may warn you. Whenever you see a message calling for immediate action, take a moment, pause and look carefully at the message. Are you sure it's real? Slow down and be safe.
- First time or infrequent senders - While it's not unusual to receive an email from someone for the first time, especially if they are outside your organisation, this can be a sign of phishing. When you get an email from somebody you don't recognize, or that Outlook identifies as a new sender, take a moment to examine it extra carefully before you proceed.
- Spelling and bad grammar - Professional companies and organisations usually have an editorial staff to ensure customers get high-quality, professional content. If an email message has obvious spelling or grammatical errors, it might be a scam. These errors are sometimes the result of awkward translation from a foreign language, and sometimes they're deliberate in an attempt to evade filters that try to block these attacks.
- Generic greetings - An organisation that works with you should know your name and these days it's easy to personalise an email. If the email starts with a generic "Dear sir or madam" that's a warning sign that it might not really be your bank or shopping site.
- Mismatched email domains - If the email claims to be from a reputable company, like Microsoft or your bank, but the email is being sent from another email domain like Gmail.com, or microsoftsupport.ru it's probably a scam. Also be watchful for very subtle misspellings of the legitimate domain name. Like micros0ft.com where the second "o" has been replaced by a 0, or rnicrosoft.com, where the "m" has been replaced by an "r" and a "n". These are common tricks of scammers.
- Suspicious links or unexpected attachments - If you suspect that an email message is a scam, don't open any links or attachments that you see. Instead, hover your mouse over, but don't click, the link to see if the address matches the link that was typed in the message. In the following example, resting the mouse over the link reveals the real web address in the box with the yellow background. Note that the string of numbers looks nothing like the company's web address.



Cybercriminals can also tempt you to visit fake websites with other methods, such as text messages or phone calls. Sophisticated cybercriminals set up call centres to automatically dial or text numbers for potential targets. These messages will often include prompts to get you to enter a PIN number or some other type of personal information.

If you receive a phishing email

- Never click any links or attachments in suspicious emails. If you receive a suspicious message from an organisation and worry the message could be legitimate, go to your web browser and open a new tab. Then go to the organisation's website from your own saved favourite, or via a web search. Or call the organisation using a phone number listed on the back of a membership card, printed on a bill or statement, or that you find on the organisation's official website.
- If the suspicious message appears to come from a person you know, contact that person via some other means such as text message or phone call to confirm it.
- Report the message to itsupport@includem.co.uk
- Delete it.