Security Awareness Training

Email Phishing

Security Awareness Modules

Awareness training modules are 5 minutes of bite sized lessons designed for all user levels to read at their own pace.

All training module follows a standard structure

- **Module -What is it**
- **Module Key Points**
- **Module Tips**
- **Module Quiz**

Security Awareness Training Modules

- **Email Phishing**
- **Passwords Management**
- **Working Outside Office**
- **Hackers**
- **Malware**
- **Email Safety**
- **Data Privacy**
- **Social Media**
- **Information Security**
- **Cyber Security**

Key Learning Objective

When you have completed all the modules you will:

- Be able to explain what Information Security, Cyber Security and Data Privacy is, and why it is so important
- Understand how and where risks can arise
- Have an awareness of some of the key things you can do to keep information secure and protected
- Know what to do if there is a problem, and who to tell
- Be able to identify an incident or a scam
- Be shown how to work responsibly inside and outside the office.
- Understand how and where cyber risks can arise
- Know what to do if there is a problem, and who to tell

There is also a short quiz designed to assess your knowledge and understanding of the subject at the end of each module

Module: Email Phishing

What is it?

Phishing emails are designed by fraudsters to appear as if they have been sent by banks, credit card companies, government departments, online stores auction sites, and other trusted organization's.

Typically, phishing emails will trick you into clicking on a link or an attachment. The link will lead you to a hoax web site that may look authentic but is where the hacker can either request confidential information such your credentials or automatically download malware such as Ransomware. By opening an attachment sent by the hacker but disguised as a legitimate file such a word or Excel document, you are actually launching a malware program such as Ransomware.

There are many different types of email phishing techniques used by hackers. The most well know and common type of email attacks are Spear Phish, BEC, CEO fraud, and General Phishing.

The Key Points

Module: Email Phishing

There are many different types of email phishing techniques used by hackers. The most well know and common type of email attacks are Spear Phish, BEC, CEO fraud, and General Phishing.
Let’s run through the 4 different categories…

BEC - Business Email Compromise Is where an attacker spoofs your company email address to impersonates a senior manager to trick you into doing something, such as transferring money to another bank account.
Spear Phishing or harpooning is similar to BEC, but the focus is typically impersonating your suppliers or partners. The end result is the same as BEC to click and download malware.
CEO / CFO Fraud Is a technique used by hackers to impersonate your company CEO or CFO and trick staff to either send money or data to the hackers
General phishing The success of a Phishing email will vary depending on the level of sophistication built into the email itself. For example, a basic spam email with limited personal information, generic in nature, poorly written and poorly, tends to get a very low click rate. Hackers use this type of email to sniff out the most vulnerable and susceptible staff.

Module: Email Phishing

The Key Points

Phishing Email Characteristics:

- The sender’s email address may be different from the trusted organization’s website address.
- The email may be sent from a completely different address or a free webmail address.
- The email may not use your proper name but uses a non-specific greeting such as “Dear customer.”
- It may contain misspelled words and poor grammar.
- A sense of urgency; for example, the threat that unless you act immediately your account may be closed
- A prominent website link. These can seem very similar to the proper address, but a single character difference can be a different website.
- A request for personal information such as username, password or bank details.
- You weren't expecting to get an email from the organization that appears to have sent it.
- The entire text of the email is contained within an image rather than the usual text format.

Module Tips

- Check the email address, name of sender before opening the email
- Check junk or spam mail folders regularly for legitimate email
- Check your spam filters are switched on
- Contact the person or organization the email claims to have been sent from if it request for example to transfer money or request confidential information
- Roll your mouse pointer over the link to reveal its destination
- Don’t respond to emails from unknown sources
- Don’t make purchases or charity donations in response to spam email
- Don’t reply to unwanted email
- Don’t unsubscribe to what you think may be phishing emails
- Encrypted personal or sensitive data before sending by email

Quiz

1. What does BEC stands for?

   a) Best email condition
   b) Business email control
   c) Business email compromise

2. You suspect you have a phishing email, what do you do?

   a) By clicking the links and or attachments you can confirm its phishing before you report it to IT
   b) Forward the email to a colleague to confirm its phishing
   c) Contact the sender by phone or ask IT to check the email

3. You need to send a confidential document to a client, do you:

   a) Encrypt it and send the password in an email with doc
   b) Encrypt it and send the password in a separate email
   c) Ensure its not encrypted so the receiver can open it

4. The following are types of email Phishing?

   a) BEC, Spear Phishing, CEO Fraud
   b) BEC, Gone Phishing, Encryption

5. Your CEO sent you urgent email to send money to a client, he also posted the bank details, but he’s not available to talk. But it must be paid today! Or else! …What do you do?

   a) Transfer the money immediately because the boss says so
   b) Wait and confirm with the CEO that it’s urgent.

Congrats you’ve completed the module!

You’re on a roll… move on to the next module