eBook: Creating a Phishing Resilient Workforce

Anyone can be a target for online scams. Use these tips to stay safe online whether you work from the office or at home.

In conjunction with our partners

Phriendly Phishing

1 Be social, but with care

Your personal information on social media can be used for targeted online scams.

How it works

- Hackers can create fake accounts to join your network
- Scammers may steal sensitive information from your social profiles (e.g. date of birth, address, etc)

Tip: Don't include your date or birth, address or other sensitive information on your social profiles

2 Don’t get caught by a phish

Many online scams start with phishing attacks.

How it works

- Scammers use fake emails to trick users into giving away access to important information or money
- Scammers may target specific individuals through ‘spear phishing’
- Scammers often buy & collect emails to use in mass scams

3 Think like a scammer

Know how scammers operate, so you can easily spot a scam!

Keep your eyes peeled for obvious signs of phishing

- Poor spelling & grammar
- A sense of urgency in the message to click or forward
- Requests for personal information or business account funds

4 Report a phish

If you receive a phishing email know how to respond.

Take these actions

- Do not click on links or attachments
- Do not respond to the email
- Notify your IT department immediately

5 Keep your details secure

Using the same password across some (or all) of your accounts can make it easy for scammers to easily access all of your accounts!

Improve your online security today

- Change your passwords to passphrases (easy to remember phrases)
- Do not use the same passphrase across multiple accounts
- Sign up to a reputable password manager to safely store your login details

ghm

Phriendly Phishing

Don’t show up at the wrong address

You check physical addresses on Maps before a trip. It’s just as important to check web URLs before you click.

How a Web Address Works

Scammers use bad web links in their attacks. Understanding the basics of a web address will help you spot fake websites and keep you and your information safe.

https: | learning. | linkin.com | /content-library

Protocol
Look for the ‘s” in https, it stands for ‘secure’. When you enter confidential information on a website, make sure the ‘s’ is shown.

Sub-Domain
This is an extension to the domain name, used to separate a website into sections.

Domain Name
This is the website address. Common domain names you might recognise are Facebook, Google & LinkedIn.

Path
The path is the exact location of a page, post or file on a website.

Can you spot the differences from above?

Here’s what a fake web address created by a hacker might look like.

http: // | linkedin_learning. | userid-86.ws | /content-library

Sub-Domain on the scam website.

Actual scam website.

Path to a fake page on the scam website.

Remember, scammers are trying to trick you.
Protect yourself. Understanding the basics of a web address will help ensure you’re not entering your username, password or credit card details on a scam website.

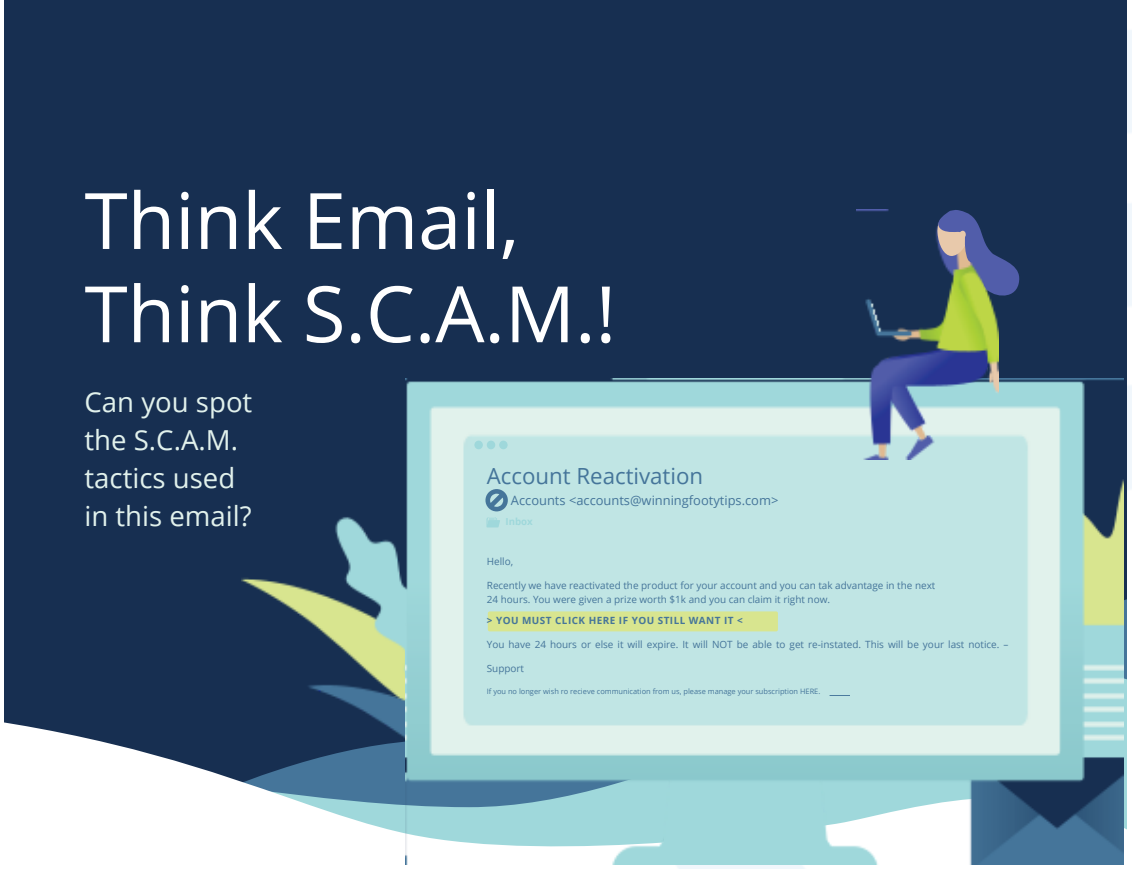
www.ghmcomms.com

ghm

Phriendly Phishing

Think Email, Think S.C.A.M.!

Can you spot the S.C.A.M. tactics used in this email?



S. Sender

Who is really sending you the email?

- An email address containing an **IP address** is probably fake.
  e.g. Microsoft@172.16.123.135
- Organisations will not use a **free email service** provider. e.g. microsoft@gmail.com
- Keep an eye out for **unusual domain names.**
  e.g. vaevk.in

A. Action

What does the email want you to do?

Be careful of clickbait tactics such as:

- **Sense of urgency** – getting you to act (or click) quickly without thinking.
- **Sense of curiosity** – the need to know or learn more.

C. Content

What's in the contents of the email?

- **Spelling & grammatical errors** can be a good indication of a phishing attack.
- Always look under **links** (Tip: hover your mouse over the link to make sure the URL is safe).
- Beware **attachments!** Check the email for signs of phishing before opening any attachments.
- Never fill out a **form** embedded in an email.

M.Manage

It's a S.C.A.M.! What should you do?

- **Don't ever respond** to a scam email.
- Don't do anything that the scam email wants you to do.
- **Notify your company's IT** service desk immediately.