Phishing is the biggest cyber threat you can face as a business, or even at home! Criminals simply cast a net in the hope that someone will "take the bait". In other words, they send out thousands of fraudulent emails knowing that it's statistically likely for someone to fall victim, whether that means clicking a link or opening an attachment. Falling victim can lead to further disruption including malware infection, account takeover, data breach, financial loss, reputational damage and much more - which is the ultimate criminal goal.

We all use email, whether that's to communicate with our colleagues, customers and suppliers; register and login to online accounts; subscribe to newsletters; and more – which makes it the perfect target. Human behaviour is much easier to manipulate than trying to break-in through dispassionate security defences.

Phishing emails pretend to be from popular brands and authoritative figures such as the government or the bank and will often reflect current trends and news such as COVID or the cost-of-living crisis. This month they will pretend to be from HMRC as we approach the end of the financial year. They manipulate emotions that will most likely cause us to respond to the email's request, often preying on a sense of urgency.

But because phishing emails are usually so generic, there are signs that can help you identify when an email is fake.

This month, we will teach you and your staff how to avoid getting caught in the criminals' net and prevent 83% of attacks towards your business. Criminals only need to be successful once, but we need to be successful all the time.

Just keep swimming…

Top 3 Tips:

- **Provide training** to all your staff to prevent them falling victim to phishing. Staff awareness improves your resilience to these attacks by 85%.
- Create a "sharing is caring" environment and **encourage staff to report all instances of phishing** to their line manager. If they have already fallen victim, you can reduce further damage; if they haven't yet then you can prevent others from the same fate.
- **Establish strong cyber resilience** to reduce harmful impacts caused by this type of crime - if

you have been following our “Getting the Basics Right” programme you will already be well on your way to achieving strong resilience!

REMEMBER to report fraud and cybercrime to Action Fraud: http://go.pardot.com/e/963723/2023-03-16/5q6dff/195724572?h=fWTD7SksduqRcTW1u4EHxD3Rs51JtNK_q_Bh9mxt1g8

We are here to help businesses like you, so if there are other ways we can achieve this please feedback to the team at info@londoncrc.co.uk or complete our short survey.

Look out for next month’s edition on Enabling Antivirus and Firewall, the next step in our “Getting the Basics Right” journey. The full timetable of the programme can be found in the Community Member’s Hub here.

Please raise awareness of the Cyber Resilience Centre for London to your fellow business neighbour. They will be eternally grateful to you when they can sleep at night knowing their business is safe and sound.

Best wishes,

Simon and Hannah

Internet Explorer 11 will be disabled

Internet Explorer 11 is no longer supported with updates, leaving the app exposed to cyber-attacks. Microsoft is slowly removing it from Windows 10 operating systems through a Microsoft Edge update. It is always recommended to use the latest version of software and operating system to remain protected from cyber-attacks.

More information can be found here.

Ransomware attacks are rife!

Ransomware attacks lock devices, filesystems and data from access, and demand a sum of money to be paid for their release. This attack can cause disruption to service, reputational damage, financial loss and data loss. It can take years to fully recover from this attack. Paying the ransom does not guarantee the malware will be removed or that the criminal will leave you be.

The National Crime Agency identified 149 British victims of ransomware strains known as Conti and Ryuk. The ransomware was responsible for extorting at least an estimated £27 million.

To protect against this threat you need simple best practices, including:

- Keep software and operating systems updated.
- Install antivirus that can detect ransomware.
- Remain vigilant of phishing emails.

- Browse the web responsibly.
- Backup your important data and assets to reduce your recovery time- make sure these backups are not contaminated with malware by keeping them off the network.
- Have an Incident Response Plan to feel ready to face this attack when it happens.

For more best practices that will reduce your risk to this threat, follow our Getting the Basics Right programme.

HMRC scam checklist

HMRC has released information to help the public identify scam emails, texts and phone calls as we approach the end of the financial year. More information can be found here.

Forward any suspicious emails to report@phishing.gov.uk and/or report to Action Fraud

- This month's webinar wrap-up will be on **Wednesday 29th March at 1pm**, summarising this month's phishing theme. Just 30 minutes of your time (with the opportunity to ask questions too). Those who attend the webinar will also be offered a **free First Step Web Assessment** worth £250 - this is an offer you don't want to miss! Register here.
- Our webinars will continue to run the last Wednesday of every month at 1pm going forward – keep this time free in your diary!
- We're also running a webinar in partnership with the Small Business Research + Enterprise Centre as part of World Backup Day. It's also on **Wednesday 29th March, starting at 2.30pm** – why not make a day of it? Register here.
- The **DCMS Cyber Security Breaches Survey 2023** will be released this Sunday 19th March at 9:30am. This publication will provide annual results from businesses, charities and educational institutions on their cyber security policies, processes and an overall assessment of resilience. Check-out the latest statistics here!
- Don't forget to check back into the Community Membership portal. We will be releasing great offers on our services but they will only be available for a select number of businesses! You can find a list of our services here.

Our Cyber Essentials Partners are a group of organisations who are supporting us in our mission to improve the cyber resilience of SMEs in London, and who we are able to recommend as providers of Cyber Essentials certifications.

Each month, we'll be a shining a spotlight on one of our Partners so you find out more about them and about what Cyber Essentials can do for your business.

This month, we're partnering with ProCheckUp, and their team of experts are helping us with technical knowledge that informs the resources we provide for you through our social media channels and Community Members' Hub.

ProCheckUp are independent cyber security experts, providing Security Audit, Compliance & Advisory, Security Risk, Incident Response and Training & Knowledge Transfer security services for over 23 years. Acting as a trusted security provider to some of the world's leading enterprise organisations and SMEs, ProCheckUp are specialists in helping customers manage risk and handle the information security challenges of today's ever-evolving threat landscape. They support small and medium sized businesses across the UK and London to develop cost-effective cyber security defences.

You can find out more about ProCheckUp here.

We're here to support you, so please reach out if there's anything we can help with.

You can find all our info through the links below ⬇

Email Website LinkedIn Twitter Facebook Instagram Youtube Forward to Friend