2-Step Verification is the saving grace for all your cyber security woes. Simply switching this on in your online account settings means criminals cannot gain unauthorised access when they scam you for your password or steal it in a data breach.

2-Step Verification is when a One-Time Passcode is needed in addition to your username and password during the login process. Because the criminal does not have access to the One-Time Passcode, your account remains safely locked.

The One-Time Passcode is often sent to your phone or generated by an authenticator app that the criminal does not have access to. If you have the option, use an authenticator app because criminals can clone your sim card to get the passcode for themselves. But having 2-Step Verification on is still more secure than only using a password for protection.

Let's look at a real-life example of a small business affected by cybercrime, who could have saved themselves the heartbreak by implementing 2-Step Verification.

A small clothes retailer had built a 10,000-strong following on Instagram, only for them all to disappear after falling victim to social media fraud. At that point, the only solution was to make a new account and start again from scratch.

2-Step Verification can seem like extra hassle, but it's also extra hassle for the criminal and therefore extra protection for you. The clothes retailer would still have their Instagram account today if they had additional security in place, but we're able to share this cautionary tale to protect you from the same fate.

One of our happy customers, a small sports retailer, had this to say:

"I now use One Time Pass Code Verification when I want to update and/or manage my website. I like that extra layer of security, and am grateful to you for suggesting it."

Top 3 Tips:

- Use an authenticator app where possible- they are free!
- Save your backup codes somewhere safe in case you lose access to your primary 2-step method.
- If the platform you are using doesn't offer 2-Step Verification, you might want to consider finding one that does.

Follow our step-by-step guides for popular platforms (you can find them in our Member's Hub!) and enable 2-Step Verification today.

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 Phishing, 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

LOOK OUT for energy rebate scams!

There have been over 1,500 reports of scams pretending to be from Ofgem offering energy rebates within 2 weeks. Remain vigilant and take a moment to consider the request. Contact the company directly using reputable details.
Forward any suspicious emails to report@phishing.gov.uk and/or report to Action Fraud.

Further information on this scam 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.

- This month's webinar wrap-up will be on Friday **24th February at 1pm**, summarising this month's 2-Step Verification 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.
- 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.

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