As our devices become obsolete and dysfunctional and we move to the latest technology, we often declutter our old equipment, but what of the data stored on them?

Data will always be your responsibility to protect so you must make sure to thoroughly wipe the device before sending it off for refurbishment or destruction. Deleting your files is simply not enough, these files can always be recovered.

When purchasing new equipment, remain vigilant for scams and make sure there is no tampering of the device before set-up.

This month we will provide you with tips on how to safely dispose of your old tech and how to effectively on-board new equipment to make sure it is resilient to cyber threats from day one.

Top 3 Tips:

- Thoroughly wipe and reset your device when disposing of old equipment, to prevent unauthorised access to data.
- Remove and destroy the hard drive and any small memory cards, etc. that hold data.

- Consider replacing insecure devices that are no longer supported by updates.

REMEMBER to report fraud and cybercrime to Action Fraud.

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 Managing User Privileges, the next step in our "Getting the Basics Right" journey.

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, and the team!

The Cyber Security Breaches Survey 2023

Have you caught up with the latest Cyber Security Breaches Survey 2023 yet? Check out the top threats businesses and charities have faced across the year and observations on the general resilience towards cybercrime - it just might give you some ideas for your own defences too!

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.

To protect against this threat, you should implement some 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.

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 24th May at 1pm, summarising this month's 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 on the **last Wednesday of every month** at 1pm going forward – keep this time free in your diary!
- Great news, we are now a **Living Wage Accredited employer**! This means that we pay a real Living Wage to all our directly employed staff, as well as any contractors we work with.
- Check out this **fantastic blog** from our Researcher Claire on How AI is impacting our ability to fight cybercrime. With the emergence of ChatGPT, an advanced language model created by OpenAI, cybercriminals have a new tool at their disposal to enhance their social engineering tactics. In this article, we will explore the impacts of ChatGPT on social engineering cybercrime and the steps that individuals and businesses can take to protect themselves.

This month, we're partnering with Forensic Control. Specialising in Cyber Security and Digital Forensics, they've provided expert and straightforward consultancy and solutions to organisations for the past 15 years: helping them assess, prevent and respond to cyber threats and incidents.

From auditing to vulnerability scanning, Cyber Essential certifications, investigation of data breaches, and IP theft, Forensic Control help their clients leave less to chance. They work in partnership with many leading Cyber Security and IT companies in the UK, and count the British Heart Foundation, Save the Children and the Church of England among their clients.

You can find out more about Forensic Control 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