POLICE DIGITAL SECURITY CENTRE

The whole world knows where you're working right now

Don't leave your home office open to cyber criminals

Top cyber security tips for working at home

1. **Strong password policy** To prevent unauthorised access to your device use a strong password for all devices and social media accounts (e.g. such as a passphrase of three random words). Change default passwords on all your devices upon initial installation (especially your *Wi-Fi router at home* or any IoT devices you may have!) and consider using password managers to store and protect your passwords.

2. **2FA** Turn on two-factor authentication on all your accounts and devices, to ensure that your data and information is secure.

3. **VPN** Use a Virtual Private Network (VPN) to have a secure link to help protect and encrypt the data you send or receive to your work colleagues while you are working at home. It will also scan devices for malicious software.

4. **Software update** Set all your devices and apps to download and install updates automatically to ensure that any crucial fixes are not missed, which will reduce the risk of your devices being infected with malware.

5. **Back up** To safeguard your most important personal data and information, back them up to an external hard drive or cloud-based storage system to avoid any losses.

6. **Phishing emails** Avoid opening links or attachments from suspicious and unexpected emails. Phishing emails may appear genuine but are embedded with a virus that could compromise your device, as well as manipulate you into sharing personal or financial information. Currently cyber criminals are exploiting the coronavirus outbreak and targeting people, as well as businesses, with fake emails around information on coronavirus.

7. **Install Anti-virus** Install and activate anti-virus software on all your devices, preferably set it to update automatically. This will help you to run a complete scan of your system and check for any malware infections.

8. **Safe online browsing** Only visit trusted websites to avoid malicious or scam websites, especially when online shopping. Keep an eye out for websites that have a padlock sign in the address bar, as this shows that the connection and your personal information (e.g. credit card information) being sent through is encrypted and secure. However, always make sure that the website is legitimate!

9. **Social media** During this time, social media might be used more often for businesses to communicate to their customers. It is therefore important to review the privacy, password and security settings for all your social media accounts to make sure they are as secure as possible.

10. **Communication** Ensure that you are maintaining contact and staying engaged with your team either via email or chat platform, as it is easy to feel isolated or lose focus when working at home.

For more useful information, NCSC has additional guidelines on working from home:
https://www.ncsc.gov.uk/guidance/home-working

Current Coronavirus-related phishing emails

Cyber criminals are targeting both the public and businesses with coronavirus-related phishing emails. These are just some of the examples that are currently circulating. Most of the emails claim to be sent by organisations or departments, such as WHO, NHS, HMRC, CDC. Please be aware of these examples, but also stay vigilant in case similar emails are being sent to you!

Tip: Always visit trusted websites and resources, for current information.

Examples

Sources: **https://www.bbc.co.uk/news/technology-51838468**
https://www.actionfraud.police.uk/alert/coronavirus-related-fraud-reports-increase-by-400-in-march

'Click here for a cure' phishing email

An email alleging to be from a mysterious doctor claiming to have details about a vaccine being covered up by Chinese and UK governments, manipulating victims to click on the attached document which will take them to a malicious website.

Covid-19 tax refund

An email claiming to be from HMRC about giving members of the public a tax rebate and manipulating the victim to click a link ('Access your funds now') that takes them to a fake government website. On the website, they encourage the user to put in all their financial and tax information.

'Little measure that saves'

An email claiming to be sent from the World Health Organisation (WHO), that has attached a document with details of how the public can prevent the disease's spread. The attached document is infected with a malicious virus called AgentTesla Keylogger, that spreads onto your computer when it is opened. This virus records every keystroke you type and monitors the victims every move online, which is sent to the hackers. Be wary of emails claiming to be from WHO, visit their official website or social media accounts instead for all of the latest advice.

'The virus is now airborne'

An email with the subject 'COVID 19- Now Airborne, Increased Community Transmission, claiming to be from the Centres for Disease Control and Prevention (CDC). The hackers managed to use the CDC's legitimate email address by spoofing it, to appear genuine. A link is attached onto the email, to encourage victims to click it and provide personal information (such as their email address and password) which will allow hackers to have control over your email account. Always turn on 2-Factor-Authentication to protect yourself.

'Donate here to help the fight'

Another fake CDC email asking for donations to develop a vaccine against coronavirus and specifically asking for donations to be made in Bitcoin.

Online Shopping Fraud

Action Fraud has reported that currently there are scams related to online shopping, where people have bought protective face masks, hand sanitisers and other essential items, online from questionable sites, which have never been delivered. Always check whether the online store you are buying from is legitimate!

Malicious Newsletters

Action Fraud also reports that cyber criminals are providing articles about COVID-19 with a link to fake company website, where victims are then encouraged to click on a malicious link to subscribe to their daily newsletter for further updates on COVID-19.

PDSC
POLICE DIGITAL SECURITY CENTRE