BPIF

EST·1901

As more of us are now working from home we thought it may be useful to look at how a few simple steps can reduce homeworkers' exposure to cyber threats. Some of these items are especially important if using personal devices.

Action	How to do this	Why it's important
Change the default password on your router	Find out the make & model of your router, and Google "how to change the default password on X"	Some routers ship with known, default passwords. This makes it easy for an adversary to access your network
Ensure you backup any data you save to your computer	You could copy items to folders on your organisation's cloud service, e.g., SharePoint/ Google Drive	Items saved to the Desktop or Documents folders aren't automatically backed up
Don't use an Administrator account when you're using the internet or email	Create a new 'standard' user and use that instead. How to do this on a Mac. How to do this on Windows	Malware can do a lot more damage when it's running under an 'Admin' account
If using your own computer, use a separate log in for work	Create a new user for example called 'Jonathan -work' on a Mac. On Windows	Keeping work data separate from home data prevents potential cross contamination
Review the apps on your computer – if you don't need it for work then remove it	Remove software on Windows. Remove app on Mac	Lots of apps are difficult to manage regarding updates & can also increase your attack surface area
Make sure you have anti-malware software running. This is important for Macs, too	Avast is a decent, free, option for Macs. By default, Windows 10 has Windows Defender, see how to check its status	Helps prevent malicious software running on your computer
Replace any easily guessable passwords with complex passwords – a unique password for each application	Give serious consideration to the use of a password manager such as 1Password, LastPass, Dashlane	If any of the websites you use suffers a breach, the attackers won't be able to use your credentials on other sites
Don't let your guard down when checking email, opening attachments	Ask yourself if you were expecting that communication; check the language of the email – is it unusually urgent?	Cyber criminals take advantage of the better side of human nature – be vigilant, check it's legitimate

While perfect security isn't possible, implementing the steps above will greatly reduce exposure to most attacks. If you've any queries on anything, or if you've any general cyber security related questions, then do please get in touch by emailing coronahelp@bpif.org.uk