Lancashire Cyber Foundry

5 Steps to Secure your New Work Computer

READ TIME: 2 MINS AUDIENCE: BUSINESS & TECHNOLOGY

It' no secret that during 2020 small and medium size business' have bought more IT equipment for homeworking. But with the number of cyber-attacks having increased 40% since 2019, many are asking how best to secure this new equipment. This article looks at 5 simple things you can do when you buy new IT equipment to make sure you're more secure.

1. UNINSTALL THINGS YOU DON'T NEED

On both Windows and Apple computers, there's a lot of free stuff that usually comes with the machine. When you first load up, have a quick look at what comes with it and ask 'What do you actually need?' Every programme you add, slightly increases the risk of an entry point of an attacker on your machines. Mostly, you have to accept that risk to use the programme you want, however if you don't use or gain no benefit from the programme the safest thing is to remove it.

2. TURN AUTOMATIC UPDATES ON

Although it's annoying, one of the purpose of updates are for the owners of the programme or software you're using to fix patches or exploits that have been revealed to them. If you miss these, you're opening a window of opportunity for hackers to exploit the uncorrected flaws in the code.

3. INSTALL AND USE MOZILLA FIREFOXOR GOOGLE CHROME

These two browsers sit in a sweet spot of being popular enough they're well supported with a range of useful plugins, whilst be very secure. Although not the most secure out there, these do offer the best usability across the internet whilst being 'secure enough'.

European Union
European Regional Development Fund

NORTHERN POWERHOUSE HM Government

Lancaster University

4. BROWSE THE BROWSER PLUGINS

Both Mozilla Firefox and Google Chrome have a vast range of plugins. It's outside of the scope of this article to suggest which would benefit your business best, however we would recommend spending time browsing the plugin libraries and seeing which suit your needs most.

5. TREAT ANY USB/ HARD DRIVE THAT ISN'T YOURS AS IF IT HAS A VIRUS ON IT

In today's age, it's rare you would need to transfer something via USB or a hard drive where it couldn't be done online. If someone suggests plugging in a USB to your system, ask if they wouldn't mind emailing it to you instead. You can see some details in an email attachment (size, file name, file type) that you can't see on a USB.

> **If someone suggests plugging in a USB to your system, ask if they wouldn't mind emailing it**

ABOUT US

The Lancashire Cyber Foundry runs a programme designed to support businesses facing cyber challenges in Lancashire. Digital Innovation support is part of this programme but there is also business stategy support available too. This includes workshops dedicated to evaluation of the driving forces which will shape the world of today and beyond. Consider how your business is affected by external changes, now consider how much time your business spends evaluating them and planning for them.

To find out more about how your business can access support or register on one of upcoming workshops contact us:
cyberfoundry@lancaster.ac.uk

ABOUT THE AUTHOR

Geraint Harries

Before starting at Lancaster University over 4 years ago, Geraint had worked in software development roles in both IBM and the Civil Service. In addition to being a qualified teacher, Geraint has worked freelance with a varied client base as a software developer and graphic designer.