Lancashire
Cyber Foundry

Are smart devices safe to use at work?

READ TIME: 2 MINS

AUDIENCE: SMALL BUSINESS

2020 saw the smart home market value hit £70bn and by 2025 its predicted to reach £110bn. The market is both diverse and competitive with an ever-growing range of smart products available from industry giants such as Amazon and Google. The Smart Connected Home Ecosystem, it here to stay. Although there's no shortage of utility and novelty, many people are starting to ask the question how safe are they in a business environment?

Broadly speaking most devices that are commercially available are required to meet certain security and privacy criteria, however they all have the same weak link that can be exploited: You! A recent study found that 90% of security breaches were due to user error.

We can define user error in two ways (1) a user actively and knowingly undermining the security of a system and (2) a user inadvertently compromising a system by inaction.

In this article, we'll concentrate on the second way and looking at some ways to overcome it.

SECURE YOUR WIFI

Consider your home or work router as the front door to your house. If you can securely lock the door, you can assume a certain level of security for all devices within the home. This applies directly with digital devices. Make sure you change your routers default password and ensure it's a secure password (not password123)

CREATE A GUEST NETWORK

Wherever you work is likely to have people coming and going and some will want to use your WiFi. If this is a regular occurrence at your business, create a guest network for these people. Treat giving them access to your work network as like giving over

European Union
European Regional Development Fund

NORTHERN POWERHOUSE
HM Government

Lancaster University

keys to your property; only when necessary and only for the specific period of time needed.

ALWAYS CHANGE DEFAULT PASSWORDS

Although we've talked about changing passwords on your router, we would also recommend changing passwords on anything with a default password.

DISABLE FEATURES YOU DON'T NEED

Having your device use the bare minimum it needs to function is the safest way to use the device. The less code on the device, the less likely it is to be exploited. For a mobile device this could mean removing unused apps, for something more complicated like a car's digital dashboard or heating system you may need to refer to the user manual and see what's required and what's surplus.

ENABLE MULTI-FACTOR AUTHENTICATION

For accounts and devices that have it, make sure you enable 2-factor authentication. This means that if someone tries to login to an account or service it will ask them to verify their legitimacy by another means, this is usually a text, but can also be an email or phone call. If you are a user who is allowed access it's an easy step to add, if you're a user who isn't allowed access, it is an incredibly hard hurdle to overcome.

FIND OUT MORE

We run a series of business strategy and cyber workshops specifically designed for SMEs in Lancashire. We're passionate about seeing Lancashire business become more cyber aware and innovative and so offer funded places for companies to come and learn how to defend, innovate and grow their business. Additionally, we have an experienced technical team ready to help you with your business innovation ideas particularly around cyber and digital innovation.

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.