Royalty-free stock illustration ID: 1155826936

Apr 30, 2021 15:07 BST

New whitepaper: how can digital footprints make us vulnerable to cyber crime?

Earlier this month, we announced our partnership with cyber security and data analytics company, CybSafe as part of our wider commitment to improving individual security habits and decreasing the number of people-related security incidents.

Alongside this, we published the first in a series of whitepapers from us and CybSafe, which explored personality traits and how these might play a part in a person's susceptibility to becoming a victim of cyber crime.

To complement this, we have released the next paper which explores whether our digital footprints can make us vulnerable to cyber crime. To dig into what this means to individuals and the organisations they work for, we spoke with Matt Lewis, commercial research director at NCC Group and co-author of the paper.

What is a digital footprint?

A digital footprint is an accumulation of our online activities – from information that is unknowingly logged, such as the web pages we visit, and the online searches we make day-to-day, to the information we willingly provide through social media or purchases we make online. The trails we create are abundant and can provide a clear snapshot of our interests, hobbies, political views and more.

How do our digital footprints contribute to an increased risk profile?

There are many factors that contribute to our susceptibility to cyber crime. From our age band to our use of tech in day-to-day life, there is a spectrum of human factors that contribute to how susceptible we are to having our data, habits and security vulnerabilities exploited by cyber criminals.

In our whitepaper, we explore how digital footprints play a role in this, breaking down the four current domains: public, private, Internet of Things (IoT) and power of the state, to demonstrate how each of these footprints are built over time. We also identify the cross-domain factors that can contribute to a greater risk profile. This includes password reuse, blurred home and work life, excessive privacy policies and readily available harvesting tools.

All of these can significantly increase the likelihood of an individual being targeted by a cyber criminal, especially in the new world of remote working which has led to a mixed use of personal and work IT.

Why is research into the human side of cyber so important?

The field of research that examines the behavioural side of cyber security is fascinating and this is why we embarked in this research project with CybSafe. By examining cyber security through a behavioural lens, we are able to gather crucial insight into what could make individuals more susceptible

to cyber crime.

The public's general awareness of the 'routes in' for cyber criminals is limited and this can have a major impact, not just on them personally, but also to the businesses they work for. Individuals and organisations must understand the relationship between personality, digital footprints and susceptibility to cyber crime, and equip their workforce with the tools and knowledge they need to minimise this risk factor.

Further research in this area will help to turn the tide against this type of crime and whilst there will always be new vulnerabilities to exploit, it'll certainly give individuals and businesses more power to tackle the problem.

What further research is needed in this area?

Our whitepapers introduce the topic at a high level and aim to bridge the technical security and behavioural science disciplines to help minimise risks associated with digital footprints.

Moving forward, we will look to explore this field of research further by investigating what personalised approaches and interventions work best for educating different users and personalities about digital footprints, and personalised approaches to minimising online risk and exposure. This will also include aspects such as the language used to communicate risk and approaches to different personality types. Essentially there is much research to be done, bridging the disciplines of cyber security and behavioural science.

If you'd like to find out more, download our research paper below.

About NCC Group

NCC Group exists to make the world safer and more secure.

As global experts in cyber security and risk mitigation, NCC Group is trusted by over 14,000 customers to protect their most critical assets from the ever-changing threat landscape.

With the company's knowledge, experience, and investment in research and innovation, it is best placed to help organisations assess, develop and manage their cyber resilience posture.

With circa 2,000 colleagues in 12 countries, NCC Group has a significant market presence in North America, Europe and the UK, and a rapidly growing footprint in Asia Pacific with offices in Australia, Japan and Singapore.

Contacts

NCC Group Press Office
Press Contact
All media enquires relating to NCC Group plc
press@nccgroup.com
+44 7824 412 405
+44 7976 234 970