The dangers lurking in our digital shadows

Ghonche Alavi describes how the digital footprints we leave behind can threaten our security and she offers advice on how to minimise the online threats

We have all heard anecdotal stories from the dark web highlighting the unsupervised horrors and goings on that are not subjected to any legal oversight. We tend to consider the dark web to be the most threatening place on the Internet. However, most people do not actually spend any time on the dark web, as they can neither access it nor know the first thing about navigating it. The surface web is where we all spend the majority of our time online and is, in fact, where we are most vulnerable.

The surface web is a great source of readily available information for our review and use. This allows us to be more efficient and at times more effective in the workplace. For instance, maybe you have a meeting set up with a potential new client – one of the first things you are likely to do is check their profile on LinkedIn. Much of the information you might want to know ahead of your initial meeting is consolidated in one place: how long they have been at the company; whether or not they are a key decision-maker in the company; what relevant qualifications they have; and so on.

Just as you have been able to source the primary school this potential new client attended in the early nineties, anyone can just as easily find out this type of personal information about you, your friends, and your family. More concerning still is the convergence between physical and information security, which means that your digital footprint, or digital shadow, can be used to gain intelligence on your daily routines. This can be used to threaten you physically.

Your digital footprint can be used to gather intelligence on daily routines, and this can be used to threaten you physically

Ikon Images | Alamy

As social media platforms continue to thrive, we are bombarded with trivial posts that reveal increasing amounts of information, as much about our own friends and family as about our acquaintances and colleagues. This is all the ammunition needed for opportunist criminals to successfully target their next victim. The attack surface has expanded as we share personal data online, on websites, platforms and applications. Consider the number of connected devices we use on a regular basis: Fitbits linked to our mobile phones or to our computers; even security cameras in and around the home connected to mobile devices and, ultimately, to systems in our homes. These are all considered fair game by hackers and criminal syndicates and your personal and private information is used to exploit you.

Opportunism

Traditionally, security concerns have been limited to physical security. In reality, in managing security threats you can no longer depend on ensuring that you build the highest fence around your house or that you install the loudest alarm with the fastest incident response team on standby. Known security breaches are shifting to the digital domain, which is laced with a number of nuanced threats. In this increasingly interconnected world, many people are able and keen to share information in real time. This is ideal for connecting and bringing people together, but it also poses a significant threat to physical and online security.

In addition to the information we willingly share online, there are many personal details that we are also inadvertently sharing. Applications with lengthy terms and conditions and excessive technical and legal jargon are often overlooked and we give little thought to how the data provided to these apps are, in turn, shared with third party providers. More importantly, we question even less how the providers of the apps secure and store the data that we have consented to sharing with them. What security configurations are in place to harden networks from intrusion by hackers? And do we care enough to stop sharing personal information in exchange for accessibility and convenience?

High-net-worth individuals and company executives are particularly vulnerable to online threats because they are appealing targets. It is no wonder that cyber criminals leverage their online vulnerability, using accessibility to their friends and family to further their goals.

For less sophisticated criminals, all it takes is a casual perusal online and suddenly there is valuable information to be leveraged. For a more sophisticated black hat hacker during the reconnaissance phase, it often becomes clear very quickly that while the targets themselves may maintain a discreet online presence, family members and their extended social circles are not so discreet. Which schools are the children enrolled at? Where does their spouse go for a morning jog? How frequently do they travel abroad? This information is often easily accessible in the early stages of reconnaissance. The individual has simply to find one weakness in their target's network; one family member or friend who has lax security controls on social media and who tends to overshare, and they are in.

While for family members, particularly younger ones, it may not be clear why so much caution should be applied when sharing information online, there are some real, tangible threats that could leave the whole family much more exposed. Small snippets of information come together and very quickly the criminal has substantial intel to act on. This can be used to plan for a wide range of crimes, from virtual kidnapping to burglary or from doxing (short for 'dropping docs', this involves breaching personal data and publishing it online with malicious intent) to mugging. Children can even become victims of cyber harassment and groomed to reveal even more sensitive information that can later be used against the family.

These crimes are financially motivated, but can have far reaching consequences, including posing a genuine physical threat, as well as having the potential to cause significant reputational damage. CRJ

What now? Ten simple steps to protect yourself online

With this gloomy picture now painted, here are ten simple steps you can take to protect yourself online:

- *Speak with family and close ones to agree on the level of information you are comfortable with sharing online. Make sure everyone understands the risks of oversharing online*
- *Avoid qualifying the nature of your relationship with others online, for example, family members or significant others*
- *Enable multi-factor authentication when possible*
- *Review all apps on your devices and ask yourself: Do you use it? Do you need it? Are you sharing the right amount of information on it? Remove unused applications on devices*
- *Avoid public WiFi when possible and when absolutely necessary use a secure licensed virtual private network (VPN) and disable automatic WiFi and Bluetooth connection*
- *Do not open emails and attachments that you were not expecting*
- *Do not use the same user name and password combination across apps*
- *Avoid using the same user name on different apps to make it harder to identify you between apps*
- *Disable automatic location sharing, especially when taking photos, to avoid geolocation being identified in the metadata*
- *If you really have to post pictures of your holiday or where you are eating breakfast, for example, do so on your return and not in real time*

Author

GHONCHE ALAVI *is a Senior Information Security Consultant at NYA, a GardaWorld company. She is a Certified Digital Forensics Examiner (CDFE) and an Ethical Hacker. Working alongside NYA's wider consulting and response teams, Ghonche supports clients before, during and after cyber incidents, working closely with forensic examiners and the crisis management team*

- *NYA is a* CRJ *Key Network Partner*
- *www.nyarisk.com*