POLICE SCOTLAND
POILEAS ALBA

Digital Footprint and Social Engineering

Cybercrime Harm Prevention

Police Scotland

04.03.25

What is a digital footprint?

A digital footprint is the data that is left behind whenever a person uses a digital service, or someone posts photographs or information about that person online. Online activities such as dating, banking, shopping, gaming, professional and social networking all add to a person's digital footprint. It is therefore likely that almost everyone will have a digital footprint.

Who contributes to a digital footprint?

It is not only you that contributes to your digital footprint. Your friends, family, colleagues, associates, and the clubs and societies you're a member of can also add to it every time they mention you online. Even people you don't know can contribute to your digital footprint. For example, corporate and public sector bodies can add to it as well, when they list public information about you on the internet. Do you know what your digital footprint looks like? It could include information about you, your home, your family and your work that others can easily gain access to without you knowing.

Managing your digital footprint

Social media websites and apps are just two examples of online services that regularly change their privacy policies and security settings, making it difficult to keep track of what's available for everyone to see and what isn't. This means that personal messages, information and data that you post online can end up being viewed by far more people than you ever intended.

You can take the following steps to manage and review your digital footprint:

1. Learn what your digital footprint currently looks like
    - Google yourself and see what information is readily available about you.
    - Be aware who else is posting about you and contributing to your digital footprint.

2. Modify your digital footprint
    - Delete old or inactive accounts.
    - Review or delete anything you have posted online that you wouldn't want everyone to know.
    - Review passwords and privacy settings on apps, devices and social media sites.
3. Manage your digital footprint
    - Be aware of automatic profile settings when setting up accounts online. These are usually set to public so anyone on the internet can view your posts, photos and status updates.
    - Be aware of apps that run analytics to monitor, collect and use your personal information for advertising purposes.
    - Don't accept friend requests off everyone, only people you know.
    - Don't constantly post your location online.
    - Ensure others know what you are and aren't comfortable with being shared online.

What is Social Engineering?

Social engineering is a targeted scam technique used by criminals in order to manipulate victims into sharing sensitive information and/or allowing them to gain access to systems. This type of attack relies on human error rather than vulnerabilities in software and operating systems which is why it is more unpredictable.

Attackers often impersonate a trusted person or organisation, such as the police or the bank. They will also utilise information they have found out about their victim online (their digital footprint) to make the scam more convincing. This is often why it's difficult to spot these scams before it is too late.

Social engineering can be quite complex and are often executed in multiple stages:

1. Investigate – Attackers do their research to pick their victim and gather background information on them from what is available online. This also allows the attacker to pick the most appropriate attack method.
2. Hook – Attackers engage with the victim in order to deceive them. They will often spin a story in order to gain victims trust and convince them real action needs to be taken, e.g. opening a link.
3. Play – The attacker executes the attack and obtains the information they want. This usually is gaining sensitive information or being granted access to systems.
4. Exit – After executing the attack, they attempt to close the interaction, trying to not leave a trace.

Types of social engineering attacks

Attackers commonly execute social engineering attacks via email, phone call, text message, or even an infected USB stick. All these methods can be adopted in order to convince victims to share personal/ financial information or allow access to systems.

Phishing, Smishing and Vishing

The attacker typically sends an email (phishing), text message (smishing) or phone call (vishing) to their target with the aim of getting snippets of information which may help with a more significant crime at a later date.

An example may be that an email is sent by the attacker who claims to be from a trusted organisation such as a bank or a shop. The fraudster may have done their background research and identified an individual's bank or shop they actually use. Since the individual trusts the organisation, it makes the message seem more convincing. The email prompts the recipient to click on the attached link, which takes them to a seemingly legitimate website of the trusted source. The target is then prompted to log into their account, during which the fraudster is collecting the user name and password.

Baiting

In the same way a fish will be attracted to a worm wriggling on a hook, the attacker dangles something (the bait) in front of the target, anticipating that it will prompt them

into taking the intended action they want them to take. The ‘bait’ could be a USB stick, memory cards, CD-ROM/DVD-ROMs or other storage medium.

For example, the attacker may leave a USB stick, which has malware loaded on it, in a location were the intended victim will find it. The USB stick may be labelled ‘Private & Confidential’ or something that will arouse curiosity/ urgency. The victim takes the bait, picks up the USB stick, and plugs it into their computer to see what is on it. The malware will then automatically install itself onto the computer and start gathering sensitive data such as emails and passwords or initiate a ransomware attack.

Email hacking and contact spamming

This plays on a person’s natural instincts to pay attention to messages from people we know. Attackers attempt to take advantage of this by taking over email accounts. This is usually achieved through guessing weak passwords, carrying out a successful phishing attack or obtaining login details as a result of large data breaches.

Once the victim’s email account has been compromised, the engineer will have access to everything including email content and the victim’s entire contacts list. These contacts will often be a mixture of friends, family and work colleagues, but may also include banks, retailers, utility companies and medical professionals.

The attacker can then create an email with either embedded malware or a phishing link and send it to the entire group of contacts. Because the email comes from a known contact, recipients are more likely to be trusting of the email, as it is from someone they know.

Pretexting

Pretexting is the use of a pretext or ploy to capture a potential victim’s attention. Once the story hooks the victim, an attempt is then made to trick them into providing something of value.

A simple example of this technique is the receiving of an email naming the potential victim as being eligible for the company bonus payment. The email requests personal and financial information to confirm the identity of the employee. The pretext is that once the victim’s identity has been confirmed, the transfer of the money into the victim’s bank account can proceed. If convinced by this pretext, the

victim will often provide the social engineer with personal information such as their bank account detail, full name, home address and date of birth.

Quid Pro Quo

This scam involves the illusion of an information exchange. An example may be the attacker, who is pretending to be an IT support technician, contacts the potential victim informing them of a technical problem or security risk on their computer.

If convinced, the victim may hand over login credentials or allow remote access to their computer, thinking they are getting a service in exchange for the handover of information. If successful, this scam allows the fraudster to take control of the victim's computer whereby personal files can be stolen or malware may be installed.

Scareware

Scareware involves victims being bombarded with false alarms and fictitious threats. Users are deceived into thinking that their device is infected with malware, prompting them to install software which claims to be able to resolve the problem. This software is malware, and it will enable the criminal to steal sensitive data or carry out a ransomware attack.

Scareware often appears as legitimate popups or banners in the victim's browser while surfing the internet. The popups will display messages such as 'Your Computer may be infected with harmful spyware – click here to remove it'.

Avoiding Social Engineering attacks

- Never reveal confidential or financial company or customer data including usernames, passwords, PINs, ID numbers or memorable information.
- Ensure that people or organisations that you are supplying payment card information to are genuine, and then never reveal passwords. No reputable organisation will ever ask you for your password via email or phone call.
- If you receive a phone call requesting confidential information, verify it is authentic by asking for a full and correct spelling of the person's name and a call back number.

- If you are asked by such a caller to cut off the call and phone your bank or card provider, call the number on your bank statement or other document from your bank – or on the back of your card – but not one given to you by the caller, nor the number you were called from. If possible, use another phone from the one you received the call on or leave it for five minutes before you make the call, in case the sender's number has been spoofed or the line left open.
- Never open email attachments from unknown sources.
- Never readily click on links in emails from unknown sources. Instead, roll your mouse pointer over the link to reveal its true destination, displayed in the bottom left corner of your screen. Beware if this is different from what is displayed in the text of the link from the email. If in doubt, call (but do not email) the sender.
- Do not attach external storage devices or insert CD-ROMs/DVD-ROMs into computers if their source is uncertain.
- Ensure your privacy settings are updated on your profile