Your digital footprints are more than a privacy risk. They could help hackers infiltrate computer networks

April 11 2022, by Ravi Sen

Your digital footprints can give hackers clues about you that they can use to trick you. Credit: Ivan/Flickr, CC BY-SA

When you use the internet, you leave behind a trail of data, a set of digital footprints. These include your social media activities, web browsing behavior, health information, travel patterns, location maps, information about your mobile device use, photos, audio and video. This data is collected, collated, stored and analyzed by various organizations,

from the big social media companies to app makers to data brokers. As you might imagine, your digital footprints put your privacy at risk, but they also affect cybersecurity.

As a cybersecurity researcher, I track the threat posed by digital footprints on cybersecurity. Hackers are able to use personal information gathered online to suss out answers to security challenge questions like "in what city did you meet your spouse?" or to hone phishing attacks by posing as a colleague or work associate. When phishing attacks are successful, they give the attackers access to networks and systems the victims are authorized to use.

Following footprints to better bait

Phishing attacks have doubled from early 2020. The success of phishing attacks depends on how authentic the contents of messages appear to the recipient. All phishing attacks require certain information about the targeted people, and this information can be obtained from their digital footprints.

Hackers can use freely available open source intelligence gathering tools to discover the digital footprints of their targets. An attacker can mine a target's digital footprints, which can include audio and video, to extract information such as contacts, relationships, profession, career, likes, dislikes, interests, hobbies, travel and frequented locations.

They can then use this information to craft phishing messages that appear more like legitimate messages coming from a trusted source. The attacker can deliver these personalized messages, spear phishing emails, to the victim or compose as the victim and target the victim's colleagues, friends and family. Spear phishing attacks can fool even those who are trained to recognize phishing attacks.

One of the most successful forms of phishing attacks has been business email compromise attacks. In these attacks, the attackers pose as people with legitimate business relationships—colleagues, vendors and customers—to initiate fraudulent financial transactions.

A good example is the attack targeting the firm Ubiquity Networks Inc. in 2015. The attacker sent emails, which looked like they were coming from top executives to employees. The email requested the employees to make wire transfers, resulting in fraudulent transfers of $46.7 million.

Access to the computer of a victim of a phishing attack can give the attacker access to networks and systems of the victim's employer and clients. For instance, one of the employees at retailer Target's HVAC vendor fell victim to phishing attack. The attackers used his workstation to gain access to Target's internal network, and then to their payment network. The attackers used the opportunity to infect point-of-sale systems used by Target and steal data on 70 million credit cards.

A big problem and what to do about it

Computer security company Trend Micro found that 91% of attacks in which the attackers gained undetected access to networks and used that access over time started with phishing messages. Verizon's Data Breach Investigations Report found that 25% of all data breach incidents involved phishing.

Given the significant role played by phishing in cyberattacks, I believe it's important for organizations to educate their employees and members about managing their digital footprints. This training should cover how to find the extent of your digital footprints, how to browse securely and how to use social media responsibly.

This article is republished from The Conversation under a Creative

Commons license. Read the original article.

Provided by The Conversation