Social engineering attacks: How to protect your business with a social media policy

Social engineering tactics

Social engineering is any technique that manipulates people to gain unauthorized access to your systems or data.[1] Hackers can gain access through a number of different social engineering techniques and exploits, including:

Workplace photo exploitation

Photo exploitation refers to the use of photographic details for malicious purposes. Even images posted by workers on their personal accounts may include sensitive papers, passwords or information in the background. Hackers may use these details to impersonate individuals and access private accounts.

False urgent emails

An attacker can create a fake email address to impersonate a manager or executive and dupe employees into clicking a malicious link, sharing passwords or paying a fake invoice for an "urgent" matter. This brand of social engineering attack can pressure employees to respond quickly before they have a chance to check the legitimacy of the request.

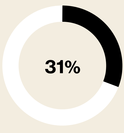
Vishing

Hackers can use sophisticated artificial intelligence (AI) to generate voice messages, potentially impersonating a boss, member of the finance team or IT professional to trick an employee into sharing financial information or passwords over the phone.[2]

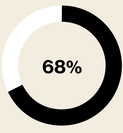
In some cases, hackers can take advantage of lapses in employee awareness. Weak passwords, for example, make it easy for cybercriminals to brute force a guess.

Why is social engineering a threat?

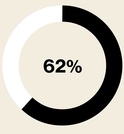
Small businesses often lack resources, robust security measures and security expertise. Social engineering attacks may target businesses and employees with various social engineering tactics, often using social media as their way in. Businesses of all sizes should consider these social engineering attack trends reported by the Verizon 2024 Data Breach Investigations Report (DBIR):



of all breaches over the past 10 years involved the use of stolen credentials[3]



of breaches involved a non-malicious human element, like a person making an error or falling victim to a social engineering attack[4]



of financially motivated incidents involved ransomware or extortion, with a median loss of $46,000 per breach[5]

increase in the number of breaches that involved the exploitation of vulnerabilities as an initial access step[6]

Protect your business with a strong social media security policy

Small steps can go a long way toward protecting your business and employees from accidentally sharing information that can lead to a breach. Here are a few tips to help you build your policy:

1. Establish some ground rules

Guidance should go beyond broad advice like "be careful." Create detailed, written guidelines on what is acceptable to post to social media.

2. Every post is important

In addition to teaching employees how to identify suspicious phone calls or emails, remind employees to take extra caution in posting from a business device, on a business social media account or in a personal post about the workplace.

3. Security is a team sport

Improve engagement and investment among your team by including them in your policymaking. This approach will help keep policies fair, inclusive and transparent while also securing the buy-in you need for success.

4. Security starts with you

Your social media security policy requires full commitment from the owner, manager and other leaders in the business.

Want to learn more about protecting your business?

Discover how Verizon Business Internet Secure helps protect your business from social engineering attacks and other threats.

The author of this content is a paid contributor for Verizon.

[1] Lossing, Marlese. "What is Social Engineering?" sdxcentral. https://www.sdxcentral.com/security/definitions/keeping-telecommuting-workforce-safe-online/what-is-social-engineering/. Accessed 18 December 2024.
[2] Ibid.
[3] Verizon, 2024 Data Breach Investigations Report, 2024, page 43.
[4] Ibid, page 20.
[5] Ibid, page 20, 9.
[6] Ibid, page 7.

verizon business