Social Engineering Attacks: protecting your small business from human manipulation

Thanks to modern technological advancements, small businesses can level the playing field with larger organisations. With access to data storage, analytics, and automation tools, small-business owners can effectively run their companies and reduce the amount of manual labour required.

Temps de lecture : minute

13 February 2024

However, this also makes them more vulnerable to social engineering attacks like phishing, pretexting, and baiting, which may not have been as common in the past. In fact, according to Barracuda, *small businesses see 350% more social engineering attacks* than enterprises, making this a serious problem that needs to be addressed immediately.

In this article, we will look at the deceptive tactics cybercriminals use and how small businesses can protect themselves against human manipulation.

What is social engineering?

Before we get started on the defense strategies, let's first *understand what social engineering is*. Social engineering is a sophisticated art of manipulation that cybercriminals use to deceive individuals in organizations. They do this by tricking people into revealing confidential information or granting unauthorised access to sensitive data. Malicious attackers often prey on human psychology by exploiting trust, fears, and

ignorance to gain access to your company's most sensitive data.

The psychology of social engineering

To effectively combat social engineering, you must be able to understand the psychology behind it. Cybercriminals often exploit our innate human tendencies by creating a sense of urgency or trust. They will then play on emotions to encourage hasty and uninformed decisions. Understanding psychological tactics is the first step to building an effective defense against sophisticated cybercriminals.

With the proper education and training, employees can become more aware of online scammers and identify any potential social engineering attempts. Most importantly, they must learn to pause and question the legitimacy of an email, call, or request before taking any action.

Countering social engineering attacks in small businesses

To protect your small business against social engineering attacks, it’s crucial to educate your employees on how to spot and handle the schemes.

- Employee Training: A well-informed workforce is the first line of defence against social engineering attacks. Train your employees to recognise phishing emails, suspicious phone calls, and unsolicited requests for sensitive information.
- Email Verification: To avoid serious security breaches, inform your team members to double-check sender addresses and verify the legitimacy of data requests before sharing sensitive information. Ensure they are also aware that some of these emails may seem urgent or come from seemingly trustworthy sources, but they should always err on the side of caution and check with a supervisor or the IT

department.
- Two-Factor Authentication (2FA): Always implement a 2FA for all your accounts and systems. Adding this extra layer of security can help you prevent unauthorised access, even if your login credentials have been compromised.
- Data Encryption: Encryption ensures that your company's sensitive data is stored and transmitted securely. This can help minimise the risk of exposure in case of any unexpected breach.

By taking these preventive measures, your small business can mitigate the risk of falling victim to social engineering attacks. It is essential to regularly review and update your security protocols and educate employees on potential threats to stay ahead of cybercriminals.

The significance of an information security plan

Having an *information security plan* in place is essential for any small business. This plan will guide how sensitive data is handled within your organization. It must outline the necessary protocols and procedures to safeguard your business's sensitive data and mitigate costly risks. A comprehensive plan should include:

Risk assessment

Conduct a risk assessment to identify potential vulnerabilities and assess the likelihood and impact of an attack on your business. By understanding your risks, you can develop targeted strategies to mitigate them and protect your business.

Backup and recovery plan

In case of a security breach, it is vital to have an up-to-date backup and

recovery plan in place. This can minimise data loss and get your business back up and running quickly, which saves valuable time and money.

Security protocols

Be sure to develop protocols for data access, sharing, and storage. You must also implement *strong password policies*, limit unnecessary access to sensitive information, and regularly review and update security measures. These protocols should also be communicated and enforced among your employees.

Beware of common scams

Now that we've covered the basics of social engineering and how to protect your small business against it, let's take a closer look at some *common scams used by cybercriminals*:

- Phishing Emails: These emails often appear to be from a reputable source requesting sensitive information, or they could even prompt you to click on *malicious links that can compromise your system*. You must train your employees to recognise and report suspicious emails to avoid this attack.
- Tech Support Scams: These scams often involve a caller claiming to be from a well-known tech company and offering to fix an issue on your computer remotely. The scammer may ask for personal information or install malware on your system. If you encounter these fraudsters, never give out sensitive information or allow remote access to your devices unless you initiate the support call and can confirm that the person contacting you is legitimate.
- Pretexting: This deceitful scam involves sending a fabricated story to the victim that tries to manipulate them into sending money, downloading malware, or sharing classified information.
- Baiting: Similar to phishing, this cyberattack involves promising free

items such as music and goods in exchange for the victim's personal information, like passwords and Social Security numbers.

- Malware: Another popular scam cybercriminals use is sending infected files as email attachments. These can be disguised as harmless documents or links, but once opened, they can install malware on your system and steal sensitive data that could compromise your business.
- CEO Fraud: This scam targets organisations by impersonating high-level executives and requesting wire transfers or sensitive information. It can be challenging to spot, so you must verify these requests for financial transactions through other means of communication and with the proper authorities.

It is essential to stay vigilant, educate your employees on these common scams, and implement strategic cybersecurity measures for your small business to prevent your company from becoming a victim. Remember, if something seems out of the ordinary, it's best to trust your instincts and take the necessary precautions to avoid being tricked by scammers.

Article by Indiana Lee