Case study

The staff at Sam's Scoops are excellent ice cream makers and make a product that is much loved in their seaside community; however, they know little about good online practices. Your task is to gather information on the do's and don'ts of online actions and then share your findings with the team. To be more specific, you'll identify three vulnerabilities, and for each one, you'll describe the risk it brings, the type of attack that a cybercriminal might use to exploit it, and a mitigation technique that can be used to reduce risk and improve safety.

Threat 1: Weak passwords

Vulnerability: Using weak passwords or reusing passwords across multiple accounts.

Risk: This increases the chances that an attacker can guess or crack the password, gaining access to the account.

Attack: Once an attacker has access to an account, they can steal sensitive data, such as personal information or financial details. They can also use the account to spread malware or launch other attacks.

Mitigation: Use strong passwords that are unique to each account. Passwords should be at least 12 characters long and include a mix of uppercase and lowercase letters, numbers, and symbols. Password managers can help you create and store strong passwords.

Threat 2: Phishing attacks

Vulnerability: Employees clicking on malicious links or opening infected attachments.

Risk: This can lead to malware being installed on the computer, which can then steal sensitive data or give the attacker control of the computer.

Attack: Phishing emails are designed to look like they are from a legitimate source, such as a bank or credit card company. The emails often contain a link or attachment that, when clicked or opened, will install malware on the computer.

Mitigation: Employees should be trained to be wary of phishing emails and to never click on links or open attachments from unknown senders. They should also keep their software up to date, as this can help protect them from malware.

Threat 3: Unsecured Wi-Fi networks

Vulnerability: Using public Wi-Fi networks without taking precautions.

Risk: This can allow attackers to intercept and steal data that is being transmitted over the network, such as passwords or credit card numbers.

Attack: When using public Wi-Fi networks, it is important to use a VPN (virtual private network) to encrypt your traffic. This will make it much more difficult for attackers to intercept your data.

Mitigation: Employees should also be careful about what information they enter on public Wi-Fi networks, such as passwords or credit card numbers. They should only enter this information on secure websites that use HTTPS.

Conclusion

In this case study, we looked at three online threats that businesses face: weak passwords, phishing attacks, and unsecured Wi-Fi networks. We discussed the vulnerabilities that lead to these threats, the risks associated with them, and how they can be mitigated.