KnowBe4

SECURITY HINTS & TIPS

Social Engineering Study Guide

Social engineering is when someone tries to manipulate you into performing an action or sharing confidential information. Unfortunately, cybercriminals use social engineering to access computer systems, gather information, or make money. Most successful social engineering attacks are caused by human error. If you familiarize yourself with common social engineering methods, you may be able to recognize and stay safe from an attempted social engineering attack. In this study guide, you can learn about social engineering and ways you can protect yourself from social engineering attacks.

Social Engineering Tricks

Cybercriminals can use several different methods to trick you with a social engineering attack. Let's go over three common social engineering methods that you may encounter and examples of each method:

Malicious Links: Cybercriminals may use malicious links to trick you into downloading dangerous software or opening an unsafe webpage. They may send you a phishing email, which is an email that may try to convince you to share sensitive information, click an unsafe link, or download a malicious attachment. For example, you could receive an email that contains a link to access shipping information for an order. Because the email seems legitimate, you may be tempted to click the link. Then, the link could download malicious software that allows the cybercriminal to control your computer.

Fake Web Pages: Cybercriminals may create fake web pages to trick you into logging into the page or entering sensitive information. For example, you could receive a phishing email that contains a link to log in to LinkedIn. Because the email seems legitimate, you may be tempted to click the link and enter your login credentials. Once you've entered your login credentials, the cybercriminal can log in to your LinkedIn account, view your personal information, and change your password so that you can't access your account.

Impersonation: Cybercriminals may impersonate a celebrity or someone you know to trick you into revealing sensitive information, clicking an unsafe link, or downloading a malicious attachment. For example, you could receive a phone call from a cybercriminal posing as your internet provider. The cybercriminal could tell you that your monthly payment is overdue and mention your account number and date of birth. Because the call seems legitimate, you may be tempted to provide your payment information. Keep in mind that impersonation attacks can also occur over email, text message, or social media.

Tips for Staying Safe from Social Engineering

Now that you're more familiar with social engineering tricks, let's go over some tips that you can use to protect yourself from social engineering attacks:

- Before clicking a link, hover your mouse over the link to make sure that the link is secure and matches the website you're looking for.
- Instead of clicking a link or a button in an email to navigate to a website, navigate directly to the website by entering the URL into your address bar.
- Before sharing sensitive information such as your birth date or your payment information, verify that the source you're sharing the information with is legitimate.
- If someone you know messages you to ask about your organization or sends you a link, call or text the person directly to make sure the request is legitimate. If a message seems suspicious, it likely is suspicious.

The KnowBe4 Security Team
KnowBe4.com