Don't Become a Victim!

Kevin Mitnick, "*The World's Most Wanted Hacker*" and KnowBe4's Chief Hacking Officer, gives you the information you need to protect yourself against the strategies and techniques hackers use to take control away from you and your organization.

DIGITAL ATTACKS

Phishing: Email-based social engineering targeting an organization.

Spear Phishing: Email-based social engineering targeting a specific person or role.

Stop, look, and think before you click that link or open that attachment.

IN-PERSON ATTACKS

USB Attacks: An attack that uses a thumb drive to install malware on your computer.

Tailgating: When a hacker bypasses physical access controls by following an authorized person inside.

Stop, look, and think before plugging any external media into your computer or allowing someone in that you don't recognize.

PHONE ATTACKS

Smishing: Text-based social engineering.

Vishing: Over-the-phone-based social engineering.

Stop, look, and think before you surrender confidential information or take action on an urgent request.

Social Engineering

Social engineering is the art of manipulating, influencing, or deceiving you into taking some action that isn't in your own best interest or in the best interest of your organization.

The goal of social engineers is to obtain your trust, then exploit that relationship to coax you into either divulging sensitive information about yourself or your organization or giving them access to your network.

Red Flags

Red flags are a sign of danger or a problem. They can be as subtle as an uneasy feeling or as obvious as an email about "suspicious charges" from a bank that you don't even have an account with.

Pay attention to these warning signs as they can alert you to a social engineering attack!

Since phishing is the most common form of social engineering, let's take a closer look at seven areas in an email and their corresponding red flags.

FROM

- An email coming from an unknown address.
- You know the sender (or the organization), but the email is unexpected or out of character.

TO

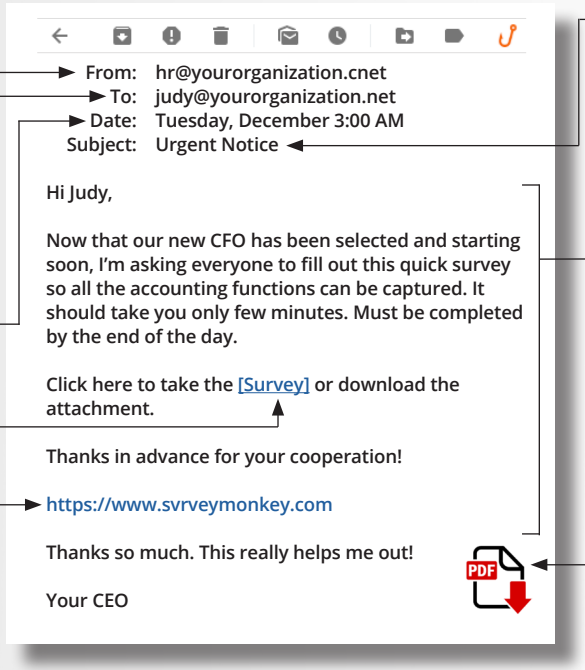
- You were copied on an email and you don't know the other people it was sent to.

DATE

- You receive an email that you would usually get during normal business hours, but it was sent at 3:00 a.m.

HYPERLINKS

- There are misspellings in the link.
- The email contains hyperlinks asking you to take an action.
- When you hover your cursor over the link, the link address is for a different website.



SUBJECT

- The subject line of an email is irrelevant or doesn't match the message content.
- It's an email about something you never requested or a receipt for something you never purchased.

CONTENT

- The sender is asking you to click on a link or open an attachment.
- The email is asking you to look at a compromising or embarrassing picture of yourself or someone you know.
- You have an uncomfortable feeling, or it just seems odd or illogical.

ATTACHMENTS

- Any attachment you receive that you aren't expecting.

KnowBe4