KnowBe4

SECURITY HINTS & TIPS

Uncovering and Reviewing Links (URLs)

You probably use URLs every day to access important websites such as your email inboxes, online banking accounts, and social media profiles. Unfortunately, cybercriminals can use URLs to direct you to malicious websites, to steal your personal information, or to initiate downloads of malware onto your devices. It's important to always think before you click so that you can protect yourself and your organization from cyberattacks.

Common URL Scams

Cybercriminals use a variety of methods to trick you into clicking on URLs. A few of the most common URL scams are explained below:

Misleading URLs: If you receive an email with information about a special deal, you may be tempted to click the link in the email to learn more. However, it's important that you stop and think before you click. Cybercriminals often include misleading URLs in phishing emails. These URLs may be disguised as links to legitimate websites, or they may be hidden by a "Click Here" link for a fake offer or promotion.

Shortened URLs: Shortened URLs are URLs that have been shortened to make them easier to view and share. These URLs are often used in marketing campaigns and for certain social media platforms such as LinkedIn. Unfortunately, these links are also convenient for cybercriminals. Cybercriminals can use URL-shortening software to hide full URLs that lead to malicious websites. Then, cybercriminals can send a shortened URL to you in a phishing email, hoping that you'll click the URL since you can't see anything suspicious about the URL itself.

Insecure URLs: When verifying that a website is safe to visit, it's important to look at the first few letters of the website's URL. Many URLs will either begin with HTTP or HTTPS. The difference between these two prefixes is that HTTPS is secure, while HTTP is not secure. Websites that use HTTPS are encrypted, which means the information on these sites is protected against unauthorized users. Websites that use HTTPS are typically more secure than other websites, but it's important that you still take precautions when using HTTPS websites, too.

Tips for Staying Safe

Don’t fall for these scams! Follow the tips below to stay safe:

- Hover your mouse over links before you click. When you hover your mouse over a link, you will be able to see the URL that you will be taken to if you click.
- If you receive an email with a link to a special deal or promotion, navigate to the organization’s website in your browser instead of clicking the link. By visiting the organization’s website directly, you can ensure that the deal or promotion is legitimate.
- Before you click a shortened URL, make sure it’s legitimate. You can use an online URL checker to view the full URL.

The KnowBe4 Security Team
KnowBe4.com