safe on social
education and consulting

www.safeonsocial.com

The danger of the link click!

With the exponential increase in internet usage, we have also seen a rise in cyber threats, including phishing, hacking, and malware attacks. One of the most common ways for these threats to infiltrate devices and, in some cases, your workplace is by clicking on suspicious links. Hence, it's essential to be mindful of the links we click on.

Check the source

Before clicking on any link, it's essential to check the source. Ask yourself, do you know the sender or the website sending the link? Is it a trusted source or a suspicious email? Sometimes, hackers use fraudulent emails that appear to be from a trustworthy source, but in reality, they are fake.

Hover over the link

Hovering over a link can give you a better idea of where it leads you. It can reveal the actual URL. If the URL seems unfamiliar or suspicious, it's best not to click on the link. Hackers may use a hyperlink that appears to be legitimate, but in reality, it takes you to a different website, where you may fall prey to phishing or malware attacks. Use caution on social media and be cautious when clicking on links shared on social media platforms, especially those from unfamiliar accounts or messages sent by people you don't know.

Verify the link

If you receive an email with a link, don't click on it right away. Instead, copy the link and paste it into a search engine. The search engine will identify the website and verify whether it's safe or not. You can also use tools like VirusTotal or URLVoid to check the link's reputation**.**

Beware of shortened URLs

URL shorteners, like bit.ly or goo.gl, are popular among hackers. They use these services to hide the actual website's URL, which may be suspicious or malicious. Hence, it's crucial to be wary of any shortened URLs you come across, especially those in emails or on social media.

Use security software

Antivirus software and firewalls can help protect your system from malicious links. They scan links and block those that are harmful. It's crucial to keep your security software up to date to ensure maximum **protection.**

Think before you click

One of the simplest yet most effective ways to avoid clicking on suspicious links is to think before you click. Ask yourself, why am I receiving this email or message? Is it something I was expecting? Does it look suspicious or too good to be true? Taking a few seconds to think before you click can help you avoid falling victim to cyber attacks.

Be cautious of urgent or threatening messages.

Hackers often use urgent or threatening language to make you click on a link. For example, they may claim that your account has been hacked and that you need to click on a link to fix the issue. Be cautious of any message that creates a sense of urgency or threatens you in any way. Instead, contact the company or organisation directly to verify the message's authenticity.

Use common sense

If something seems too good to be true, it probably is. Be cautious of any message that promises something too good to be true, such as a free holiday, quick ways to make money or free products. Remember, if it seems too good to be true, it probably is.Unpredictability: Create a unique password without easily guessable patterns or sequences, making it harder for hackers to predict.