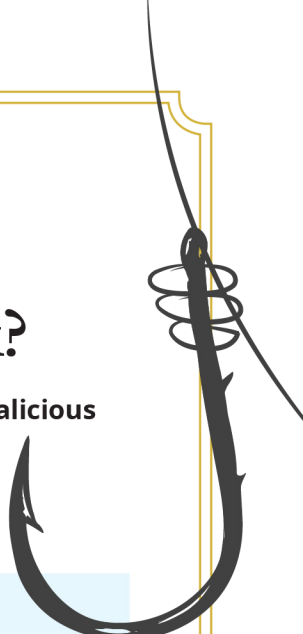


What Happens When You Click on A Phishing Link?

A cornerstone of cybersecurity is not clicking on phishing links or downloading malicious attachments. But what happens if you do? Here are a few potential consequences:

- 
- 1 You become a high-profile target.**
By clicking on a phishing link, you confirm for the attacker that 1) you're a real person, and your email is current, and 2) you're gullible. The attacker might use this information to build a profile about you and sell it to other attackers, who will then send much more threatening phishing emails. You could also experience a major increase in spam.
 - 2 You have personal information stolen.**
In a lot of cases, a phishing link will direct you to a webpage that looks legitimate. The page will ask you to enter various types of personal information like your full name, email, username, password, and so on. If you proceed, you effectively hand over your identity to a criminal, who can use this information to open fraudulent accounts in your name.
 - 3 You lose control of your accounts.**
Let's say you're logged into your bank account when you click on a phishing link. This may allow cybercriminals to run an exploit known as session hijacking. Meaning, they could intercept the communication between the bank's website and your computer and take control of your account. If successful, they will now have all the same access you have, allowing them to transfer money, change passwords, and steal personal data.
 - 4 You infect your device with malware.**
In more insidious phishing attacks, clicking on a link or downloading an attachment could result in malicious code that corrupts your device, steals data or, worse yet, infects your computer with ransomware. Ransomware is of particular concern here at work because it could encrypt our data or lock our systems until a ransom is paid, leading to both a loss in revenue and expensive downtime.

All of these scenarios are just examples of what could happen. Regardless of severity, falling for a phishing scam must be avoided no matter what. Remember, cybercriminals often cast wide nets with generic phishing emails that feature the typical, easy-to-spot red flags. But some attacks are much more sophisticated and may appear to come from someone you know, such as a co-worker or manager.

Use extreme caution when handling messages (including those on mobile devices) that contain links, attachments, and requests for information or money. As a rule, if you're unsure, don't click! And report all phishing attacks immediately.