PHISHING FUNDAMENTALS

What Happens When You Click?

Like most scams, phishing uses human emotions to get a response. The attacker wants you to do something against your best interests: click on a link, download an attachment, or send sensitive information. They convince you to do this by creating a false sense of urgency, such as offering large sums of money, threatening you with late fees, or claiming that your account has been locked due to fraudulent activity.

What happens when you click on a phishing link?
We have a few examples:

You give away your personal information.

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 send that data to a criminal, who can use it to open fraudulent accounts in your name.

You lose control of your accounts.

Let's say you're logged in to your bank account when you click on a phishing link. Cybercriminals may be able to run an exploit known as session hijacking. This allows them to intercept the communication between the bank's website and your computer and take control of your account. If successful, they will gain the same access you have, allowing them to transfer money, change passwords, and steal personal data.

Your device gets infected with malware.

In some 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 to your employer. It could encrypt your company's entire data or systems until a ransom is paid. This expensive downtime and loss in revenue could be crippling.

These are a few examples of what could happen. We hope you can see why you want to avoid falling for a phishing scam.

How to spot phishing attacks

Carefully review each email you receive:

- Are you familiar with the sender?
- Does it contain poor grammar or misspelled words?
- Are there any suspicious links or unexpected attachments?
- Does the message offer unrealistic promises, like large sums of money?
- Does it plead with you to click on a link, download something, or send personal information?
- Does it threaten you by saying an account has been hacked or that you face legal action?

An answer of yes to any of these questions is a major red flag. The email may be a scam!

First Midwest Bank
BANK WITH MOMENTUM