Microsoft Security

# 4 ways to protect yourself from phishing

Phishing is a type of fraud where criminals try to get information or access through deception and trickery. Fraudsters will pretend to be a business or person you trust in hopes you'll click on the malicious link.

## Common phishing attacks

### Content injection

This type of phishing attack injects a familiar website, such as an email login page or an online banking portal, with malicious intent. This can include a link, form, or pop-up that directs users to a secondary website, where they're asked to input confidential information.

### Link manipulation

A phishing fraud can sometimes come in the form of a malicious link that appears to come from a trusted source, like big companies and famous brands. If the link is clicked, it takes users to a spoofed website, where they are prompted to enter account information.

### Email

Phishing emails are the most prevalent form of phishing attacks, targeting both personal and professional email addresses. These deceptive emails often contain instructions to follow, malicious links to click, infected attachments to open, or an embedded QR code, all designed to trick the recipient into divulging information or downloading harmful software.

### Man-in-the-middle

Man-in-the-middle phishing attacks occur when a cybercriminal tricks two people into sending information to each other. The scammer may send fake requests or alter the data being sent and received by each party.

### QR Codes

QR code phishing stemmed from an increased use of QR codes during Covid-19. Now phishing emails can include a malicious QR code, or you may scan a malicious QR code posted in a public place. Once scanned, these QR codes can direct users to deceptive websites intended to gather their login information, or download malware or spyware to their mobile devices, which can compromise personal information and potentially take control of the devices.

**Falling for a phishing attack can lead to leaked confidential information, infected networks, financial demands, corrupted data, or worse, so here's how to prevent that from happening:**

**1**

Be careful about clicking unexpected links and emails, especially if they direct you to sign into your account. To be safe, log in from the official website instead.

**2**

Avoid opening email attachments from unknown senders or friends who do not usually send you attachments.

**3**

Install a phishing filter for your email apps and enable the spam filter on your email accounts.

**4**

Be skeptical of QR codes you receive via email or that you find. Try to preview the URL or visit the official website instead.

Explore more cybersecurity awareness topics and skilling opportunities at https://aka.ms/cybersecurity-awareness.

Microsoft Security

©2024 Microsoft Corporation. All rights reserved. This document is provided "as-is." Information and views expressed in this document, including URL and other internet website references, may change without notice. You bear the risk of using it. This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes.