Top 9 phishing scams to watch out for in 2024

By Joel Lee, Senior Editor, PCWorld Jul 10, 2024

Phishing scams have been around since 1995, but they're always evolving. Here's what you need to know about the different types and how to spot them.

Phishing is one of the most popular techniques used by cybercriminals to break into your accounts, steal your data, and even infect you with malicious software like ransomware. According to the 2024 Phishing Report by Zscaler ThreatLabz, there were 58.2 percent more phishing attacks globally in 2023 than in 2022, showing that phishing isn't just alive and well—it's still growing and evolving.

Looking to keep your computer safe from outside threats? Check out PCWorld's roundup of the best antivirus software available right now.

Keep reading to learn what phishing is, what the different types of phishing scams are, and how to identify them.

What is a phishing scam?

Phishing is a social engineering scam in which a cybercriminal tries to trick you into giving away sensitive data (e.g., login credentials, credit card details, etc.) or installing malware on your computer. It gets its name from "fishing" due to its similarity of technique: the cybercriminal lures you with bait and hopes you'll bite, not realizing that you've taken the bait until the hook is already in you.

There are several types of phishing scams—the lures, the hooks, the targets might vary from scam to scam, but the idea is the same. Here are the different phishing scam types and what you need to look out for so you don't accidentally fall for one.

1. Email phishing

In **email phishing**, someone sends you a fake email that looks very much like an official email, hoping to trick you into clicking a link or button. These fake emails tend to imitate popular companies with products or services you're likely using such as Amazon, Google, LinkedIn, or PayPal. The most commonly spoofed company, though? Microsoft.

The emails may try to scare you into action, perhaps claiming that your account has been locked or that you've been charged thousands of dollars. The goal is simple: if you're alarmed, you're likely to rush and act without thinking, making you more likely to fall for it.

2. Spear phishing

Spear phishing is a particular kind of email phishing that targets a specific individual and incorporates personal information into the attack in order to make the target more likely to believe it's legitimate.

For example, a spear phishing attacker may claim to be part of your company's IT department and ask you to confirm your login credentials. Or they might send you a fake invoice to be paid out. Or they might pretend to be your boss and ask for sensitive information.

By incorporating familiar details in the email (e.g., your boss or a client you previously worked with), the hope is that you'll lower your guard and treat the entire message as trustworthy.

3. Whaling

Whaling is a special type of spear phishing that targets high-profile individuals for big leads and payouts. Common victims include senior executives, CFOs, and CEOs who have enough power to access privileged data or move around large amounts of money.

These attacks have to be more sophisticated than normal phishing attacks, but the results can be huge: theft of trade secrets, financial loss in the millions, or even access to secure systems and networks.

4. Calendar phishing

Have you ever received an unsolicited Google Calendar or Outlook event invite? If so, you've been hit by **calendar phishing**.

Calendar phishing is a technique that uses online calendar invites to trick you into clicking malicious links embedded within those invites. It's less common than email phishing, but more dangerous because you're less likely to be suspicious of calendar invites.

It's especially dangerous if you use a calendar app that automatically adds invites to your calendar. Never click links inside unsolicited calendar invites, and make sure to disable any auto-add features.

5. Quishing (or QR code phishing)

What's your reaction when you see a QR code in the wild? Are you compelled to scan it and see where it takes you? Think twice before you do… because it could be scam bait.

Quishing (also known as **QR code phishing**) is a type of phishing that preys on this compulsion. And since scanning a QR code is basically the same as clicking on a link, the risks are the same—and these dirty QR codes can appear anywhere.

For example, the QR code on a parking meter could be replaced with a fake one that leads you to a scam site where you're tricked into entering payment information. Or you might receive an innocuous flyer in the mail with an innocent-looking QR code that leads to a virus.

QR codes can also appear in regular phishing emails in place of links, except you can't "hover over" them to see where they lead. It's why quishing is becoming more popular among hackers.

6. Smishing (or SMS phishing)

Whereas most phishing attempts happen by email, **smishing** (or **SMS phishing**) is what it's called when it happens via text messages.

Smishing attempts commonly impersonate trustworthy sources, including banks, government agencies, and popular retailers. You'll get an unsolicited text message asking you to click on a link.

One popular smishing scam pretends to be USPS (or any other courier) and asks you to click a link to resolve a failed delivery. Other smishing scams involve promises of free products, personal inquiries, or warnings that your account will be closed if you don't act now.

To protect yourself, ignore text messages from unfamiliar numbers and never click links in SMS—even from people you know.

7. Vishing (or voice phishing)

Scammers may also try to phish for victims using automated phone calls, which is why this technique is called **vishing** (or **voice phishing**).

In a vishing attempt, you might receive an unsolicited phone call—usually from a spoofed number that mimics a real person's number—that tries to scare you with legal action or financial problems. Some vishing attempts will even leave voicemails for you.

For example, one popular vishing tactic right now claims to come from a law firm with an open case against you, threatening that this supposed case will proceed if you don't call them back ASAP.

Most vishing attempts will try to scare you into paying hundreds or thousands of dollars, while others may be trying to coax personal details from you so they can steal your identity.

8. Deepfake phishing

A deepfake is a video that's been artificially modified so that the likeness of the person in the video has been swapped with the likeness of someone else. More simply, it's a doctored video that shows someone doing something that they aren't actually doing.

These highly realistic deepfake videos can be used to trick, threaten, and coerce *you* into doing something *you* don't want to do (or revealing details you don't want to reveal). Hence, **deepfake phishing**.

For example, your boss might send a video asking you to make a big payment to a new account, except your "boss" is a hacker hiding behind a deepfake. Some hackers can even do real-time deepfakes and trick you through Zoom video calls, while others may clone the voice of someone you know (e.g., a relative) and try to scam you via phone call.

9. Angler phishing

If you're on social media, you need to be aware of **angler phishing**, which is when someone impersonates an official social media account and tries to get you to click a link or divulge sensitive information.

For example, if you complain about Amazon on Twitter, an attacker might impersonate Amazon Support and reach out to you privately about resolving the issue—but what they really want is for you to give up your personal information and/or login credentials.