TWINTEL

Don't Be Phish Bait: Outsmart Phishing & Online Scams

What Is Phishing?

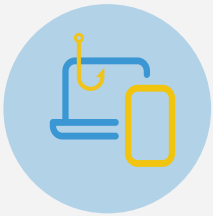
Phishing attacks usually come in emails, text messages, or phone calls that appear legitimate but contain malicious links or attachments. Once a victim clicks on the links their data is at risk of being compromised.

Verify Sender

If an email address looks off or has a different format than other emails from that sender, it's a red flag. Look out for character swapping, like Os for 0s.

Stay Alert

Keep an eye out for other signs of phishing, including urgent language, strange attachments, too-good-to-be-true offers, and poor grammar or formatting.



Confirm Situation

If you're unsure about the validity of a message, contact the supposed sender using another communication method to see if there is actually an issue.

Don't Respond

Reliable senders won't ask for sensitive credentials over insecure channels. If a message asks for personal, financial, or login information, do not respond.

Common Types of Attacks

Email Phishing: Harmful links, attachments, or requests for money and data are sent via email.

Smishing: Suspicious text messages, often appearing to be from a bank, include malicious links.

Vishing: Scammers call targets and trick them into revealing personal or financial information.

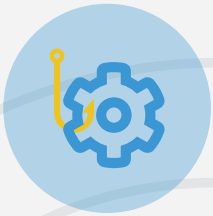
Angler Phishing: Attackers use social media messaging, comments, and posts to deceive users.

Spear Phishing: Personalized attacks on specific individuals or organizations.

Whaling: Phishing aimed at high-profile targets like executives, seeking sensitive data or money.

Check URLs

Before ever clicking on an unfamiliar link, hover your mouse over it. Check the URL in the bottom left corner of your screen to make sure it's legitimate.



Be Proactive

Use strong network management methods like firewalls, endpoint protection, and frequent software updates. Install spam filters on email platforms.