iSecurify

Phishing & Social Engineering Attacks

Phishing and Social Engineering Attacks

Awareness is the key to prevention and mitigation

What is Phishing?

Phishing is a kind of social engineering attack. Criminals send messages that look legitimate, trying to trick you into giving up sensitive data or downloading malicious software.

How Common is it?

Phishing is one of the most prevalent kinds of cyberattacks. Over 255 million incidents were observed over a six-month period in 2022, part of a 217% percent increase from 2021.

Can You Prevent It?

Some phishing attacks get caught in firewalls and filters built into your IT environment. Make sure those are installed and always be on your toes to catch any that slip through the cracks.

Tell-tale Signs

Phishing emails often come from unknown senders and have misspellings or other errors in the subject line, the sender's address, and elsewhere. If you see any of these warning signs in your inbox, there's a chance someone is trying a phishing attack. Contact IT immediately.

Plenty of Phish!

Phishing attacks are also extremely varied in nature. One of the most dangerous kinds is **spear phishing**, which targets specific people with personal details. There are also voice and **SMS phishing** schemes that can target other communication channels via your smartphone.

Protect Yourself

Ultimately, employee awareness and vigilance are what prevent phishing attacks from succeeding. Never open an email or download an attachment unless you can verify the sender. And never click a link someone sends you unless you can verify the domain is safe.

Want to learn more about preventing phishing?

Get in touch!