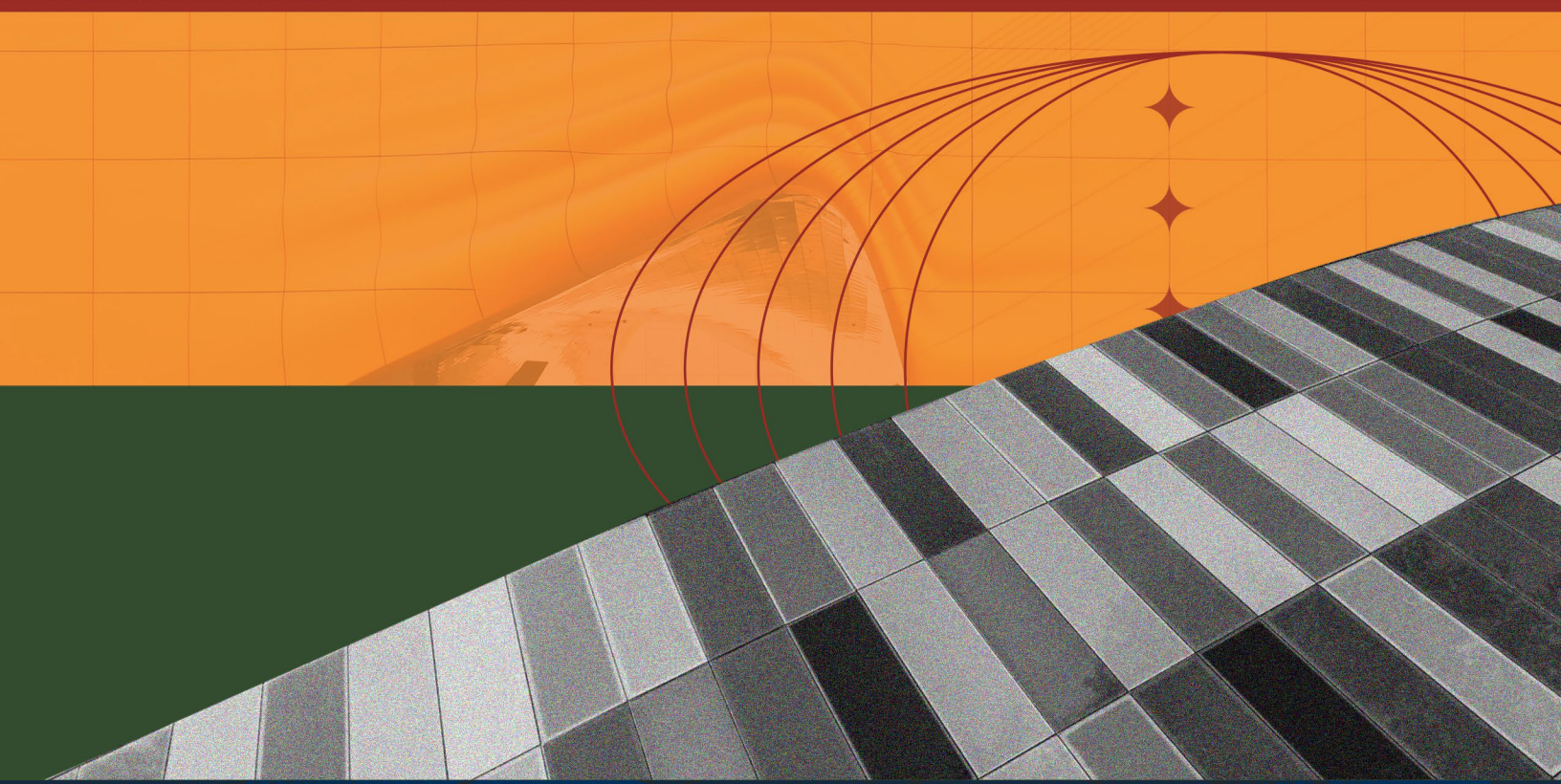
Phishing and Social Engineering Attacks

RSI Security



858.999.3030 | info@rsisecurity.com

2024

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!

www.rsisecurity.com • 858.999.3030 • info@rsisecurity.com

The latest stats

Phishing attacks continue to be a significant cybersecurity threat worldwide. Here are some of the latest statistics:

[Volume of Attacks]

In the first quarter of 2024, the Anti-Phishing Working Group (APWG) reported 963,994 phishing attacks, marking the lowest quarterly total since Q4 2021. This is a notable decrease from the 1,624,144 attacks observed in Q1 2023.

APWG Docs

[Targeted Sectors]

Social media platforms were the most frequently attacked sector in Q2 2024, accounting for 32.9% of all phishing attacks.

APWG

[Business Email Compromise (BEC)]

The average wire transfer amount requested in BEC attacks in Q1 2024 was $89,520, an increase from the previous quarter. Notably, 72.4% of all BEC scams utilized Google Gmail accounts.

APWG

[Employee Susceptibility]

A 2024 report by KnowBe4 revealed that, on average, 34.3% of untrained employees were prone to phishing attacks. However, after 90 days of training, this percentage dropped to 18.9%, and further decreased to 4.6% after a year of ongoing training.

KnowBe4 Blog

[AI-Driven Phishing]

The integration of artificial intelligence has led to a 1,265% surge in phishing emails and a 967% increase in credential phishing since late 2022. Cybersecurity professionals express significant concern over AI's role in enhancing the sophistication of phishing attacks.

Investopedia

[Global Impact]

A survey conducted in September 2024 found that nearly 45% of employed individuals worldwide have fallen victim to cyberattacks or scams, compromising personal information such as banking or email accounts.

New York Post

These statistics underscore the evolving nature of phishing threats and the critical importance of continuous vigilance and training to mitigate risks.

www.rsisecurity.com • 858.999.3030 • info@rsisecurity.com