CROWDSTRIKE
business resilience

Best Practices

Security Awareness: Phishing

Phishing is the most prominent method of infiltration for cybercriminals, who use it to insert malicious links, viruses and ransomware into an organization. A successful phishing attack can result in loss of company data, compromised credentials and accounts, and financial impact. Educating employees about phishing helps improve the company's security posture.

Identifying a Phishing Attack

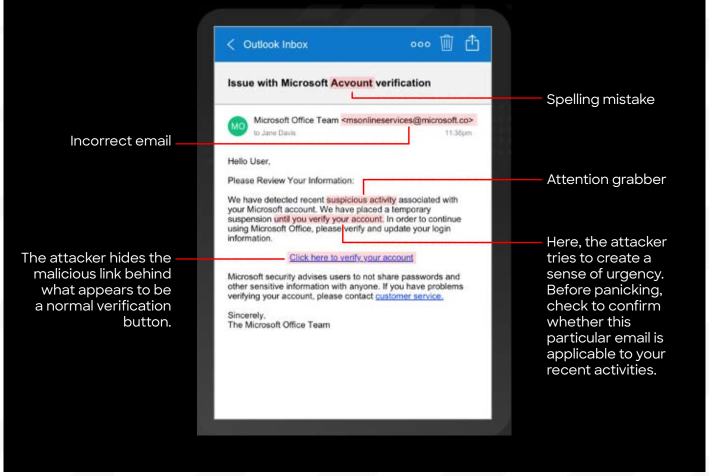
Many phishing attacks include a generic message, but some attacks may include personalized information in an attempt to appear legitimate (known as spearphishing). The attacker may attempt to mimic legitimate websites and convince users to click a malicious link or download an attachment, taking advantage of people’s trust or lack of awareness.

In phishing scams, attackers often impersonate high-profile brands and organizations such as delivery companies, financial institutions, healthcare systems and government agencies.

Always check the legitimacy of the sender. Does the sender's email address look correct? Is the message generic? Are there grammatical errors? Are you being pressured to take action immediately? Consider hovering over any link within the email to see if the link address looks legitimate.

Phishing Example

This email is not targeted and fairly generic


Outlook Inbox
Spelling mistake
Incorrect email
Attention grabber
Here, the attacker tries to create a sense of urgency. Before panicking, check to confirm whether this particular email is applicable to your recent activities.
The attacker hides the malicious link behind what appears to be a normal verification button.

Issue with Microsoft Acvount verification

Microsoft Office Team <msonlineservices@microsoft.co>
to Jane Davis 11:36pm

Hello User,

Please Review Your Information:

We have detected recent suspicious activity associated with your Microsoft account. We have placed a temporary suspension until you verify your account. In order to continue using Microsoft Office, please verify and update your login information.

Click here to verify your account

Microsoft security advises users to not share passwords and other sensitive information with anyone. If you have problems verifying your account, please contact customer service.

Sincerely,
The Microsoft Office Team

In 2023, phishing emails totaled **1.76 billion**, the highest amount on record. This represents a **51% increase** from 2022.

Source: Vade, Phishers’ Favorites: 2023 Year-in-Review, https://www.vadesecure.com/en/phishers-favorites-2023-ebook

Identifying a Phishing Attack *(continued)*

Attackers use social engineering to trick people into giving up valuable information. Adversaries may use multiple means of communication to gather information, such as emails, text messages, phone calls and social media. This information gathering may take place over a long period of time.

Vishing is a form of phishing that uses voice calls over the phone. It is often well-rehearsed and usually involves a seemingly routine interaction (e.g., a tech support issue or bank transfer). Vishers will attempt to socially engineer their target and use highly effective techniques to persuade victims to reveal specific information or perform an action for illegitimate reasons. Attackers will pose as a reputable entity or person, and artificial intelligence (AI) can allow them to more realistically impersonate familiar voices, making this attack vector even more difficult to detect.

Reporting an Attack

Be aware at all times of potential phishing attempts. Making a habit of reporting a phishing attack creates a safe environment in an organization. Employees should be made aware of the different ways of reporting suspicious emails.

Methods of reporting a phishing attack:

- If your company provides a Report Phishing button in your email application, use it whenever you think a message could be a social engineering attempt. It’s always better to over-report than under-report. If in doubt, report it.
- Forward a suspicious email as an attachment to your company’s phishing desk or help desk, following your company's policy. This may not be possible for mobile devices, but you should still forward it to your company’s phishing desk or help desk, following your company's policy.
- If a phishing attack comes via a text message, take a screenshot and send it to the phishing desk or help desk.

Methods of reporting a vishing call:

- Notify your company’s incident response team or help desk, following your company’s policies.

Get more resources from CrowdStrike for creating your own Security Awareness Program →

About CrowdStrike

CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with the world’s most advanced cloud-native platform for protecting critical areas of enterprise risk — endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: We stop breaches.

Learn more: https://www.crowdstrike.com/

Follow us: Blog | X | LinkedIn | Facebook | Instagram