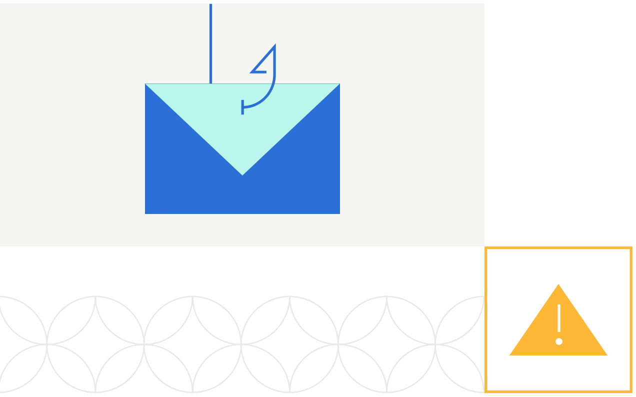
Phishing Education at a Glance

7 Warning Signs and How to Respond



Phishing is a social engineering attack where threat actors impersonate legitimate users or businesses to trick users into taking action. And phishing works — Coalition claims data showed phishing was the initial attack vector for 76% of reported claims in 2022.

How to use this guide

Our digital world moves fast, creating opportunities for human error, which can lead to cyber incidents. Threat actors know this, and they exploit it. We created this guide as an education resource to help organizations defend against this very common and potentially destructive email phishing attacks.

1. Start by reviewing the nonexhaustive warning signs of a phishing email. It focuses on how you may spot a phishing email, and how you can attempt to verify the authenticity of the message.

2. Next, take a look at the nonexhaustive list of recommended technical controls that can help prevent phishing attacks. Keep in mind that the right set of controls will depend on the size of an organization, and the maturity of their IT or security teams.

Insurance products are offered in the U.S. by Coalition Insurance Solutions Inc.("CIS"), a licensed insurance producer and surplus lines broker, (Cal. license # 0L76155) acting on behalf of a number of unaffiliated insurance companies, and on an admitted basis through Coalition Insurance Company ("CIC") a licensed insurance underwriter (NAIC # 29530). See licenses and disclaimers.

WARNING SIGN	HOW TO RESPOND
Sense of Urgency	To ensure users take action, phishing emails often use urgency such as requesting an immediate payment or transfer of information to complete a time-sensitive task. Pause before acting on urgent email requests, especially unexpected ones, and confirm with the sender.
Inconsistent email or domain	Often phishing emails make use of spoofed or fraudulent domains, making it important to review email addresses and URLs carefully. Inconsistency or misspellings may indicate a fraudulent website or email address. For example, john@abcc.com instead of john@abc.com
Unexpected attachments	As a best practice, avoid opening attachments, especially if the file extension is commonly associated with malware (.zip, .exe, .scr, and others). Confirm with the sender or your IT department before downloading. Don't be afraid to raise your hand if you make a mistake. Always report downloads that appear suspicious or alter the behavior of your system.
Requests for payments or information	To avoid invoice manipulation, never accept new or payment change information via email. As a best practice, implement a dual control process to verify payment instructions or requests using a known good phone number — threat actors can, and do, include phone numbers they control in phishing emails.
Unfamiliar tone or content	Similar to spelling and grammar errors, exert caution when emails contain an inconsistent tone or content. For example, your CEO's urgent email or text requesting gift cards is suspicious, especially if they've never made a similar request.
Spelling or grammatical errors	While generative AI and writing assistant tools make it less likely for phishing emails to contain egregious spelling and grammar errors, users should remain on the lookout.
Spoofed email or domain	Spoofed websites and emails can look identical to a valid email or website. Inconsistencies in tone, writing style (to include spelling and grammar), and requests may serve as clues of this more advanced phishing technique.

Coalition, Inc. · 55 2nd Street, Suite 2500, San Francisco, CA 94105 · help@coalitioninc.com

Insurance products are offered in the U.S. by Coalition Insurance Solutions Inc.("CIS"), a licensed insurance producer and surplus lines broker, (Cal. license # 0L76155) acting on behalf of a number of unaffiliated insurance companies, and on an admitted basis through Coalition Insurance Company ("CIC") a licensed insurance underwriter (NAIC # 29530).

Sometimes, a well-crafted phishing email can sneak through. Organizations should foster a culture of security awareness and encourage employees to report clicking on phishing links.

A layered combination of phishing awareness and technical controls can help minimize the damage from clicking a malicious link, and stop threat actors from disrupting business operations. The following technical controls can help organizations safeguard against phishing attacks.

TECHNICAL CONTROL	HOW IT HELPS
Multi-factor Authentication (MFA)	You may have heard username and passwords described as keys to the kingdom. Once stolen via phishing, threat actors use them to gain access to your organization's network. MFA (a combination of something you have, something you know, or something you are) adds another layer of authentication, requiring users to input a code or verify via an application that their access request is legitimate.
Role-based Access Control (RBAC)	RBAC helps organizations implement the principle of least privileged access by separating user accounts from administrator accounts and granting privileges appropriately. This limits access to critical business data, and ideally prevents a threat actor from gaining complete network access. Mature organizations may consider implementing a zero trust network access (ZTNA) model.
Email security: Sender Policy Framework (SPF)	SPF is a record you can add to your domain name system (DNS) settings that specifies what mail servers are allowed to send email on your domain's behalf. SPF helps to ensure that someone cannot create an email server and send it from your domain unless you have authorized them to do so in your DNS records.
Email security: DomainKeys Identified Mail (DKIM)	DKIM ensures that emails sent to and from your mail server haven't been altered in transit. DKIM is configured through your mail provider and is free.
Email security: Domain-based Message Authentication, Reporting and Conformance (DMARC)	DMARC ties SPF and DKIM together with another simple DNS record that provides a policy for how SPF and DKIM operate. DMARC also specifies an email address where delivery and forensic reports can be sent for analysis.

Continued →

Insurance products are offered in the U.S. by Coalition Insurance Solutions Inc.("CIS"), a licensed insurance producer and surplus lines broker, (Cal. license # 0L76155) acting on behalf of a number of unaffiliated insurance companies, and on an admitted basis through Coalition Insurance Company ("CIC") a licensed insurance underwriter (NAIC # 29530). See licenses and disclaimers.

TECHNICAL CONTROL	HOW IT HELPS
Implement email filtering	Email filtering can filter inbound and outbound traffic to scan and potentially avoid the delivery of harmful messages. There are a variety of email filtering techniques, including scanning for viruses and malicious code, or more robust reputation based blocklists (RBL). GSuite Business and Office 365 support email filtering, and commercial tools can be layered to provide advanced email filtering protection.
Password management	Reused usernames and passwords can present unique security risks, and threat actors will attempt to use stolen personal credentials to access business assets. Enforce good password hygiene by implementing a strong password policy and using a password manager to organize and protect user credentials.
Security awareness training	Humans are often the weakest element in any organization's security stack. Security awareness training can teach employees what to look out for and remind them to always report suspicious emails, text messages, and instant messages.

Keep threat actors away by taking Control of your cyber risk

Staying one step ahead of hackers requires vigilance, but cybersecurity doesn't have to be daunting with Coalition ControlTM.

Control is Coalition's cyber risk management platform powered by Coalition's Active Risk approach to help clients detect, assess, and mitigate risks before they strike.

Log into Control for additional cybersecurity insights and risk management tips, customized to your organization's risk profile. Control also has a growing Marketplace of cybersecurity partners that offer capabilities in areas such as multi-factor authentication (MFA), endpoint detection and response (EDR), security training, phishing simulations, and more.

Insurance products are offered in the U.S. by Coalition Insurance Solutions Inc.("CIS"), a licensed insurance producer and surplus lines broker, (Cal. license # 0L76155) acting on behalf of a number of unaffiliated insurance companies, and on an admitted basis through Coalition Insurance Company ("CIC") a licensed insurance underwriter (NAIC # 29530). See licenses and disclaimers.