








Incident Preparedness Toolkit: Phishing

Phishing occurs when threat actors trick users into taking action and can easily lead to business-interrupting cyber claims, such as ransomware and funds transfer fraud (FTF). This is your guide to spotting some of the most common warning signs of a phishing attack and how to partner with Coalition on the road to recovery. If you're looking for pre-claim guidance on how to prevent future cyber incidents, visit our guide linked [here](#).



| WARNING SIGN | HOW TO RESPOND |
|---|--|
|  Sense of urgency | <p>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.</p> |
|  Inconsistent email or domain | <p>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.</p> |
|  Unexpected attachments | <p>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.</p> |
|  Requests for payments or information | <p>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 call the last known valid phone number of the requesting organization — threat actors can, and do, include phone numbers they control in phishing emails.</p> |
|  Unfamiliar tone or content | <p>Similar to spelling and grammatical errors, exercise caution when emails contain an inconsistent tone or content. For example, your CEO's urgent email or text requesting gift cards is suspicious, <i>especially</i> if they've never made a similar request.</p> |
|  Spelling or grammatical errors | <p>While generative AI and writing assistant tools make it less likely for phishing emails to contain egregious spelling and grammatical errors, users should remain on the lookout.</p> |
|  Spoofed email or domain | <p>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.</p> |

How to protect against phishing attacks

Suggested steps as follows:

Sometimes, a well-crafted phishing email can sneak through. Technical and policy controls can help mitigate the risk of a full-blown incident, and Coalition pre-claims assistance can help determine next steps after you've clicked a phishing link.

- 1 Implement multi-factor authentication (MFA) for all accounts
- 2 Control user access to information — especially financial and critical business data
- 3 Secure your email using free or low-cost tools (SPF, DMARC, DKIM)
- 4 Use email filtering to reduce the number of phishing attempts
- 5 Implement a strong password policy and never reuse passwords
- 6 Hold security awareness training and encourage users to report suspicious emails

How to work with Coalition after a phishing attack

Experiencing a cyber event can be overwhelming, but Coalition is your partner in the recovery process. Seek guidance without the fear of triggering a claim — we can help you triage any suspected event and minimize impact, potentially preventing the threat actor from launching other, more serious attacks.

Our Claims team is available 24/7 and will begin the process of triage and connecting you with the appropriate vendors. Upon further investigation from our team, we can determine what happened and how to mitigate similar incidents in the future

Once our team has handled the expenses incurred and recovered your systems to the fullest extent possible in accordance with your policy, you're on your way to putting this incident behind you and returning to your business — better prepared.

Contact Coalition right away. You can reach us 24/7 by phone, email, or live chat.

PHONE

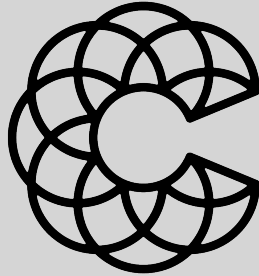
US & Canada: 1 (833) 866-1337
UK: 0808 134 9559

EMAIL

US & UK: claims@coalitioninc.com
Canada: claims@coalitioninc.ca

LIVE CHAT

Available via our [website](#)



Coalition[®]

COALITIONINC.COM

COALITION INSURANCE SOLUTIONS, INC.

44 MONTGOMERY STREET, SUITE 4210, SAN FRANCISCO, CA 94104

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 # OL76155) 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](#).

Incident response services provided through Coalition's affiliate Coalition Incident Response (CIR) are offered to policyholders via panel selection.

Copyright © 2024. All rights reserved. Coalition and the Coalition logo are trademarks of Coalition, Inc.