



BREAKING ALERT:



Chubb Vulnerability Alert System - “Protecting Against Sophisticated Vishing and IT Impersonation”

Chubb provides alerts to keep our policyholders informed of risks that may affect their organizations.

Chubb has noted an increase in social engineering attacks leveraging email bombing followed by voice-phishing, or “vishing,” tactics targeting employees across geographies, industries and all size organizations. One such campaign features a targeted email bombing whereby a threat actor (TA) sends multiple emails containing common phishing characteristics (e.g., malicious links, misspellings, grammatical errors, etc.), followed by phone calls from the TA claiming to be an IT Help Desk employee. The TA will then provide instructions for downloading a remote management tool or enabling remote desktop. Microsoft Teams, Slack, and Zoom have also been leveraged by threat actors to communicate directly with employees, often impersonating internal IT support personnel.

Chubb recommends the following best practices to reduce the likelihood of falling victim to sophisticated social engineering tactics:

- Enforce least privilege to prevent unauthorized software downloads
- Block access to known remote management tool sites (e.g., Action1, AnyDesk, Atera, ConnectWise/ScreenConnect, GoTo Resolve, MeshCentral, NetSupport Manager, PDQ Connect, Remote Utilities, RemSupp, RustDesk, SimpleHelp, Splashtop, Supremo, Syncro, Tactical RMM, TeamViewer, etc.)
- Harden Microsoft Teams, including blocking and/or restricting external domains and personal accounts. Apply the same hardening configurations and identity verification protocols to requests received via Slack, Zoom, or any collaboration platform.
- Never provide your password or approve a sign-in prompt unless you have initiated a Technology support request.
- Be cautious of unexpected calls or emails claiming to be from the Help Desk, especially if they appear urgent or if you have not requested Technology support.
- Verify caller identity before sharing any information, even if the caller ID appears legitimate. Message the individual directly through Teams or other approved communications tools and wait for confirmation before proceeding.
- Reject unexpected MFA push notifications and report them to your Security team immediately.
- When contacting the Help Desk, reference or request a support ticket number to validate the legitimacy of any IT interaction.
- If something does not feel right, hang up and contact your Help Desk or IT support personnel directly via a published Help Desk phone number, not a number provided by the caller.
- Report any suspected vishing or social engineering attempts to your Security Operations Center (SOC) or security team immediately, even if you are uncertain whether an incident occurred.

Chubb’s Cyber Risk Advisory Team is available to answer your questions and help mitigate cyber exposures like the ones described above. To request advisory services, please [click here](#).

For additional information on Chubb’s advisories, visit Chubb’s cyber threat intelligence [website](#) or please contact cyber@chubb.com. You may also use Chubb’s interactive tool [Chubb Cyber Index®](#) to access additional resources to help evaluate and address cyber risks your business may face.

[Learn more about Chubb's Cyber Services.](#)



Chubb's cyber insurance policyholders are monitored using non-intrusive outside web scanning methods. While these methods vary and are subject to change, the insights generated are typically viewable in cybersecurity rating company reports, such as those provided by BitSight and Security Scorecard, which all Chubb cyber policyholders have complimentary access to review. For more information about vulnerability alerts and our scanning technology or to sign up, click [here](#) ; or contact Chubb's Cyber Global Risk Advisors at cyber@chubb.com. Chubb makes no representations or warranties around these continuous monitoring efforts, and cannot reasonably alert all policyholders about all observed vulnerabilities. For more thorough service, consider speaking with a Managed Security Service Provider.

Chubb is the marketing name used to refer to subsidiaries of Chubb Limited providing insurance and related services. For a list of these subsidiaries, please visit our website at www.chubb.com. The materials and information contained herein are distributed for informational purposes only by ACE American Insurance Company on behalf of itself and its U.S.-based affiliates. The information provided is advisory in nature and is offered as a resource to be used together with your professional insurance, technical, legal, and other advisors in maintaining a cyber loss prevention program. The information provided should not be relied on as technical, insurance, or legal advice or a definitive statement of the law in any jurisdiction. For such advice, you should consult your own legal counsel, technical advisor, or insurance consultant. No liabilities or warranties are assumed or provided by the information contained in this email or document or in other information provided by Chubb's Cyber Risk Advisory Team. You are under no obligation to contract for services that may be recommended or with any of the service providers. Adoption of a recommendation or vendor is your independent choice. Neither Chubb nor its employees or agents make any warranties or assume any liability for the recommendations or the performance of any vendor, including any goods or services received. Before you adopt a recommendation or engage with vendors, you should conduct your own due diligence to ensure the company and its services meet your needs. Unless otherwise indicated or approved, payment for services provided by any vendor is your responsibility.

Chubb, 202 Hall's Mill Road, Whitehouse Station, NJ 08889-1600. This email (including any attachments) is intended for the designated recipient(s) only, and may be confidential, non-public, proprietary, and/or protected by the attorney-client or other privilege. Unauthorized reading, distribution, copying or other use of this communication is prohibited and may be unlawful. Receipt by anyone other than the intended recipient(s) should not be deemed a waiver of any privilege or protection. If you are not the intended recipient or if you believe that you have received this email in error, please notify the sender immediately and delete all copies from your computer system without reading, saving, printing, forwarding, or using it in any manner. Although it has been checked for viruses and other malicious software ("malware"), we do not warrant, represent, or guarantee in any way that this communication is free of malware or potentially damaging defects. All liability for any actual or alleged loss, damage, or injury arising out of or resulting in any way from the receipt, opening or use of this email is expressly disclaimed.

This promotional message was sent by Chubb, 436 Walnut Street, Philadelphia, PA 19106

©2022 Chubb. All rights reserved.

[Unsubscribe](#) | [Privacy Statement](#) | [Terms of use](#) | [View in Browser](#)