



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 one described above. To request advisory services, please [click here](#).

For additional information, 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.



Click here to 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, 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.

All content in this material is for general information purposes only. It does not constitute personal advice or a recommendation to any individual or business of any product or service. Please refer to the policy documentation issued for full terms and conditions of coverage.

All Cyber Services are subject to change. Changes to the service offerings will be displayed on the local Cyber Services web form. Policyholders are responsible for reviewing the specific terms and conditions of each Cyber Service provider to ensure eligibility and remain informed regarding any changes. The complimentary cost is applicable only to policyholders who are net new subscribers/customers to the respective services.

The services referenced are provided by a third-party vendor not affiliated with Chubb. The fact that offers and potential discounts may be made available by the third-party vendor is not an indication that insurance coverage is available under any Chubb policy for any particular incident. Discounts on products and services offered by this vendor are available only to Chubb policyholders with current in-force policies and are subject to applicable insurance laws. For products and services provided, the policyholder and third-party vendor would enter into a vendor relationship directly. Chubb will not be involved in the policyholder's decision to purchase services and has no responsibility for services that may be provided.

Chubb European Group SE (CEG). Operating in the UK through a branch based at 40 Leadenhall Street, London EC3A 2BJ. Risks falling within the European Economic Area are underwritten by CEG which is governed by the provisions of the French insurance code. Registered company number: 450 327 374 RCS Nanterre. Registered office: La Tour Carpe Diem, 31 Place des Corolles, Esplanade Nord, 92400 Courbevoie, France. Fully paid share capital of €896,176,662.