CHUBB®

September 2026

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.

UK9136-HS 02/26