International Authorities Warn of COVID-19 Cybersecurity Threats

PUBLISHED ON
April 13, 2020

Two top-level international cybersecurity authorities have teamed up to warn the world about cyber criminals exploiting the remote workforce.

The U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) and the UK's National Cyber Security Centre (NCSC) issued a joint alert last week warning individuals and organizations of the types of scams used by cyber criminals. It also provides role-specific mitigation strategies and guidance to avoid falling victim during these vulnerable times.

The joint alert reports that cyber criminals are expected to continue to use a variety of ransomware and other malware over the coming weeks and months to exploit the pandemic. Threats observed by the organizations include all of typical modes of compromise, but using COVID-19 as the "lure." These include phishing (targeting both email and text message platforms), distribution of malware through a variety of means, and registration of new domain names using words related to COVID-19. Threats also include targeted attacks against newly-created and expanded remote access and teleworking infrastructure - including the exploitation of popular online meeting platforms like Zoom and Microsoft Teams.

The alert offers the following tips for spotting phishing communications sent by cyber criminals:

- Criminals often pretend to be someone important to you. Does the email/text sender have the **authority** they claim to have? Are they really your bank, doctor, lawyer, or government agency?
- Criminals often make threats of fines or negative consequences and want you to act with **urgency**. Are you told you have a limited time to respond?
- Criminals will try to evoke **emotion** by making false claims against you or otherwise try to pique your curiosity. Does the message cause you some level of panic or provoke you to some action?
- Criminals know there is a **scarcity** of certain resources and that we sometimes have a fear of missing out. Is the message offering something of short supply?

The alert also offers the following tips to help defend against hijacking of online meetings:

- Do not make online meetings "public" - instead require a meeting password and use the "waiting room" feature (for Zoom).
- Do not share a link to the meeting on social media.

- Change settings in these platforms to only allow the host to share their screen.
- Make sure you are only using the most updated versions of the meeting software.
- Ensure that use of these platforms meet the requirement of your organization's policies and obligations (contractual and regulatory) regarding information security.

The joint alert also provides information technology professionals with access to resources regarding COVID-19-related malicious cyber activity, including summaries of "indicators of compromise" and general advice and tips on combatting the threats. In addition to making sure non-tech employees are aware of the threats and are educated on defending against these attacks, the joint alert reminds these professionals of their responsibility to take a four-layer approach to their mitigation strategies:

- Make it technically difficult for criminals to reach individual users.
- Help individual users identify and report phishing communications.
- Protect the organization from phishing emails that individual users will fall victim to.
- Respond quickly to incidents.

The joint alert emphasizes that the cyber-related threats posed by COVID-19 are fast-moving. As a result, organizations and their employees must remain alert to increased activity and take the proactive steps to protect themselves and their organizations.

If anyone has any questions on cybersecurity in this time of a remote workforce, contact me or any member of the Barley Snyder Cybersecurity Service Team.

DISCLAIMER: As we face an unprecedented time of legal and business uncertainty, we are working to provide updates on the status of important legal news related to COVID-19. It is important to note that the situation is changing rapidly and the information provided in our alerts is not intended to create an attorney-client relationship. The information contained in our alerts is for general informational purposes only and should not be construed as legal advice or a substitute for legal counsel. If you have questions about your legal situation or about how to apply information contained in this alert to your situation or about how any other information found on our website may affect your business, you should reach out to one of our attorneys. We assume no responsibility for the accuracy or timeliness of any information provided herein or by any linked site. As information changes rapidly, users are strongly advised to verify any information before relying upon it.

WRITTEN BY:

Donald R. Geiter, J.D., M.S.L. (Cybersecurity Law & Policy), CIPP/US, CIPM

Partner

Tel: (717) 399-4154

Email: dgeiter@barley.com