WINSTON & STRAWN LLP

BLOG

Multinational Response to Malicious Online Activities Related to COVID-19

APRIL 14, 2020

On April 8, 2020, a multinational alert was issued, warning individuals to remain vigilant for COVID-19-related malicious cyber activity. The warning was jointly issued by the Cybersecurity and Infrastructure Security Agency (CISA) at the U.S. Department of Homeland Security (DHS), and the UK's National Cyber Security Centre (NCSC).

Both CISA and NCSC report a growing use of COVID-19-related themes by malicious cyber actors against individuals and organizations of all sizes. Additionally, the rapid increase of remote workers has in some cases led to the use of less secure services, further increasing the risk that bad actors may gain access to sensitive information. In particular, efforts to exploit popular online platforms, video tools, and virtual networks are increasing in number as companies have quickly transitioned to partial or full remote work environments. NCSC has further observed phishing attempts being carried out through text messages, especially with respect to messages that purport to link to information about government aid.

CISA and NCSC recommend that organizations take the following steps to protect themselves, and continue to remain alert and aware of the threat of this fast-moving COVID-19-related malicious cyber activity:

- **Make it difficult for attackers to reach your users.** This includes using secure platforms, services, and end-user devices, and ensuring that telework policies address requirements for physical and information security.
- **Help individuals identify suspicious communications by educating them about common schemes that cyber attackers use to induce individuals to click on emails or provide sensitive information.** This includes claims that the communication comes from someone with authority (*g.*, a government agency or bank); has urgent timing (*e.g.*, a limited time to respond); incites emotion, like panic or curiosity; or offers something that is in scarce supply (*e.g.*, medical cures or money).
- **Teach individuals to be on the lookout for signs of other possible attacks.** This includes raising awareness about spoofed log-in sites for email or government services, instructing individuals to carefully review URLs before clicking on them, and refraining from clicking on attachments that originate from unfamiliar sources.
- **Use extra precautions when utilizing online meeting services.** This includes making meetings private, requiring a password for access, refraining from publicly sharing meeting links (*e.g.*, on social media), enabling controls to give the host the ability to control entry into meeting and screen-sharing settings, and using the most up-to-date versions of these platforms.

- **Create a security incident response plan to enable a quick and efficient response to any incidents.** Note that existing procedures may need to be adjusted to account for a remote workforce.

If you have further questions, contact your Winston relationship attorney for more information. View all of our COVID-19 perspectives here. Contact a member of our COVID-19 Legal Task Force here.

2 Min Read

Authors

Sara Susnjar

Alessandra Swanson

Related Locations

Chicago | London

Related Topics

COVID-19 | Data Breach

Related Capabilities

Privacy & Data Security

Related Regions

North America | Europe

Related Professionals

Sara Susnjar

Alessandra Swanson

This entry has been created for information and planning purposes. It is not intended to be, nor should it be substituted for, legal advice, which turns on specific facts.

© 2024 Winston & Strawn LLP.