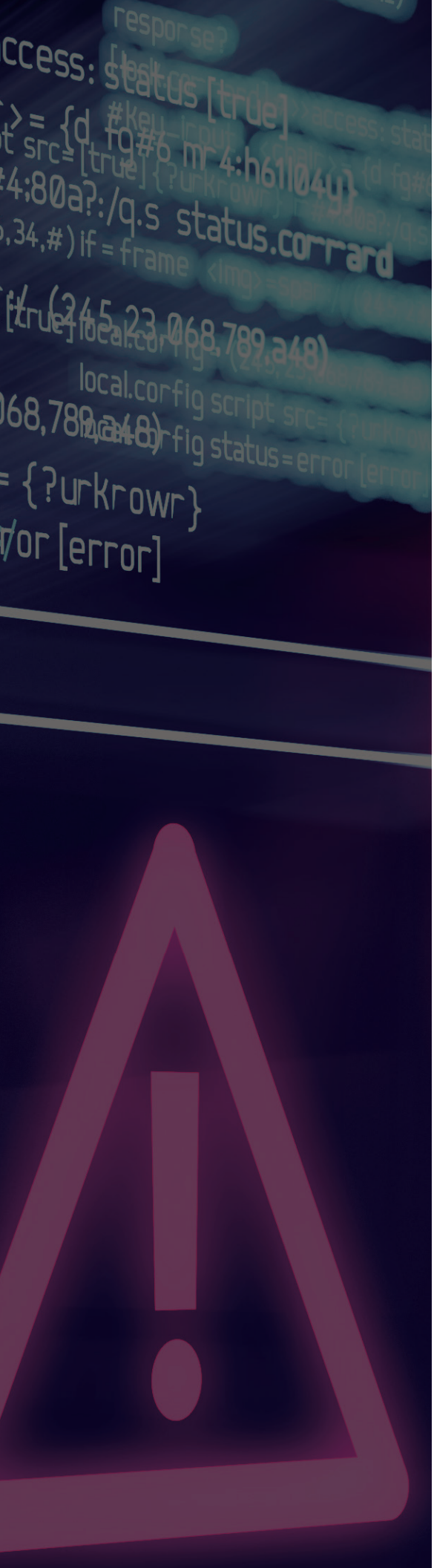

# Cyber Criminals Seeking to Capitalize on Coronavirus

Criminals prey on unfortunate circumstances, seeking to capitalize on victims during times of panic and hardship. Unfortunately, the coronavirus disease 2019 (COVID-19) pandemic is no exception.

The Cybersecurity and Infrastructure Security Agency (CISA), part of the U.S. Department of Homeland Security, told individuals to be vigilant about scams related to COVID-19.

Cyber criminals have been known to pose as charities or legitimate websites to lure victims into sending money or revealing personal information. Individuals should scrutinize any email, text or social media post related to COVID-19 and be cautious when clicking any links or attachments.

CISA offered specific guidelines for individuals to avoid being scammed online:

- Avoid clicking links from unsolicited emails, and be wary of email attachments.
- Use trusted sources when looking for factual information on COVID-19, such as CDC.gov.
- Never give out personal or financial information via email, even if the sender seems legitimate.
- Never respond to emails soliciting personal or financial information.
- Verify a charity's authenticity before making any donations.

It's not always easy to disregard messages from senders that seem reputable, like banks. If individuals have any doubts about an email from a seemingly legitimate source, they should navigate to the organization's website and use the contact information there to reach out. Individuals should never respond to the initial message.

***If individuals have any doubts about a message's sender, links or attachments, they shouldn't click anything in the message.***

## What Can Employers Do?

Employers should consider notifying employees about the existence of these COVID-19 cyber scams. Especially during times of crisis, scammers will pose as reputable sources and use fear to solicit personal information. Employers should also communicate best practices so employees know how to respond to such solicitations.

It may also benefit employers to back up data and bolster network protections in case an employee clicks the wrong link and compromises the entire system.

Speak with Cottingham & Butler for more cyber security guidance.

**Tips to secure your organization in a work-from-home environment:**
https://www.sans.org/blog/tips-to-secure-your-organization-in-a-work-from-home-environment/

**Security Awareness Work-from-Home Deployment Kit:**
https://www.sans.org/security-awareness-training/sans-security-awareness-work-home-deployment-kit

Access Cottingham & Butler Client Resource Center