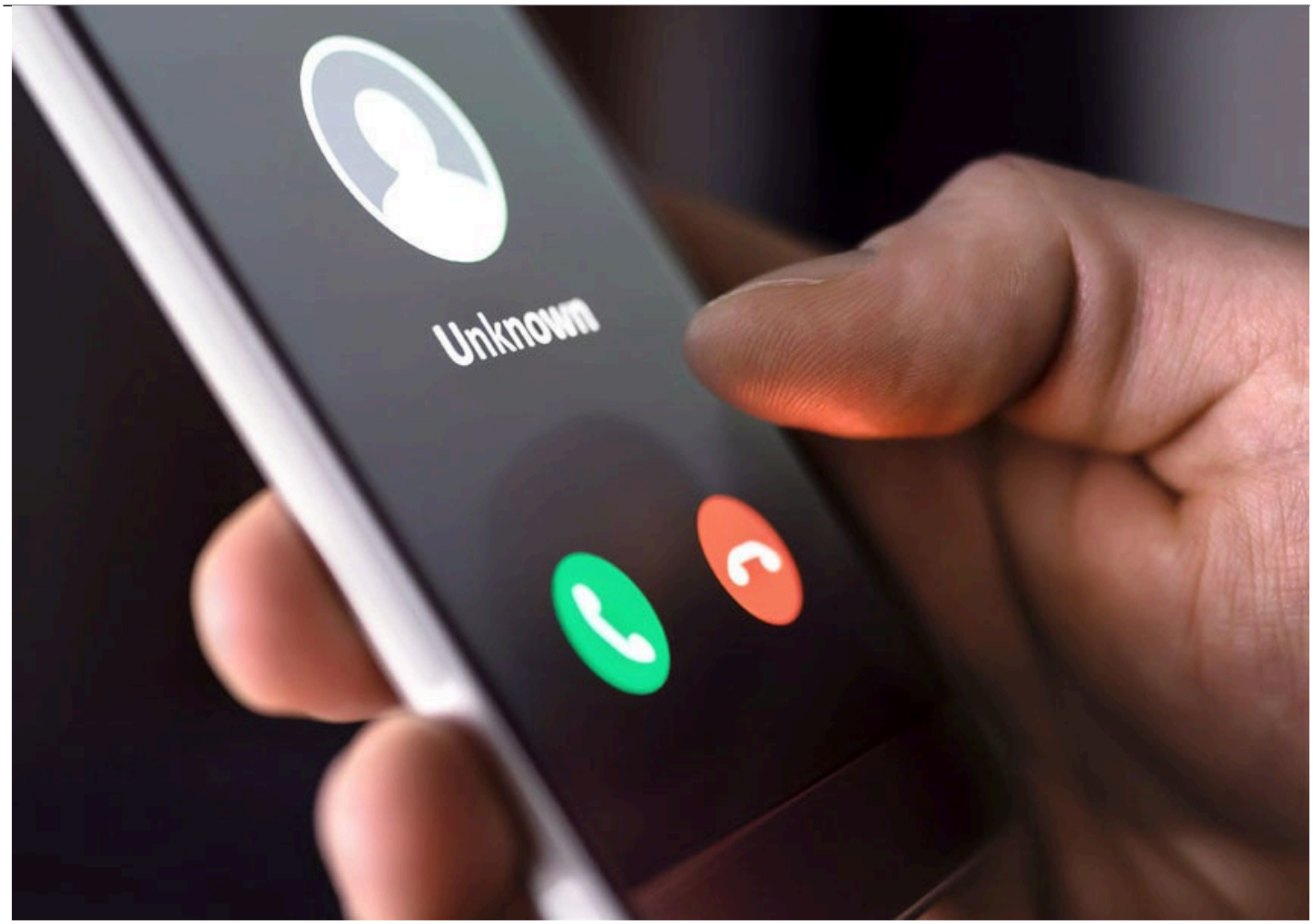
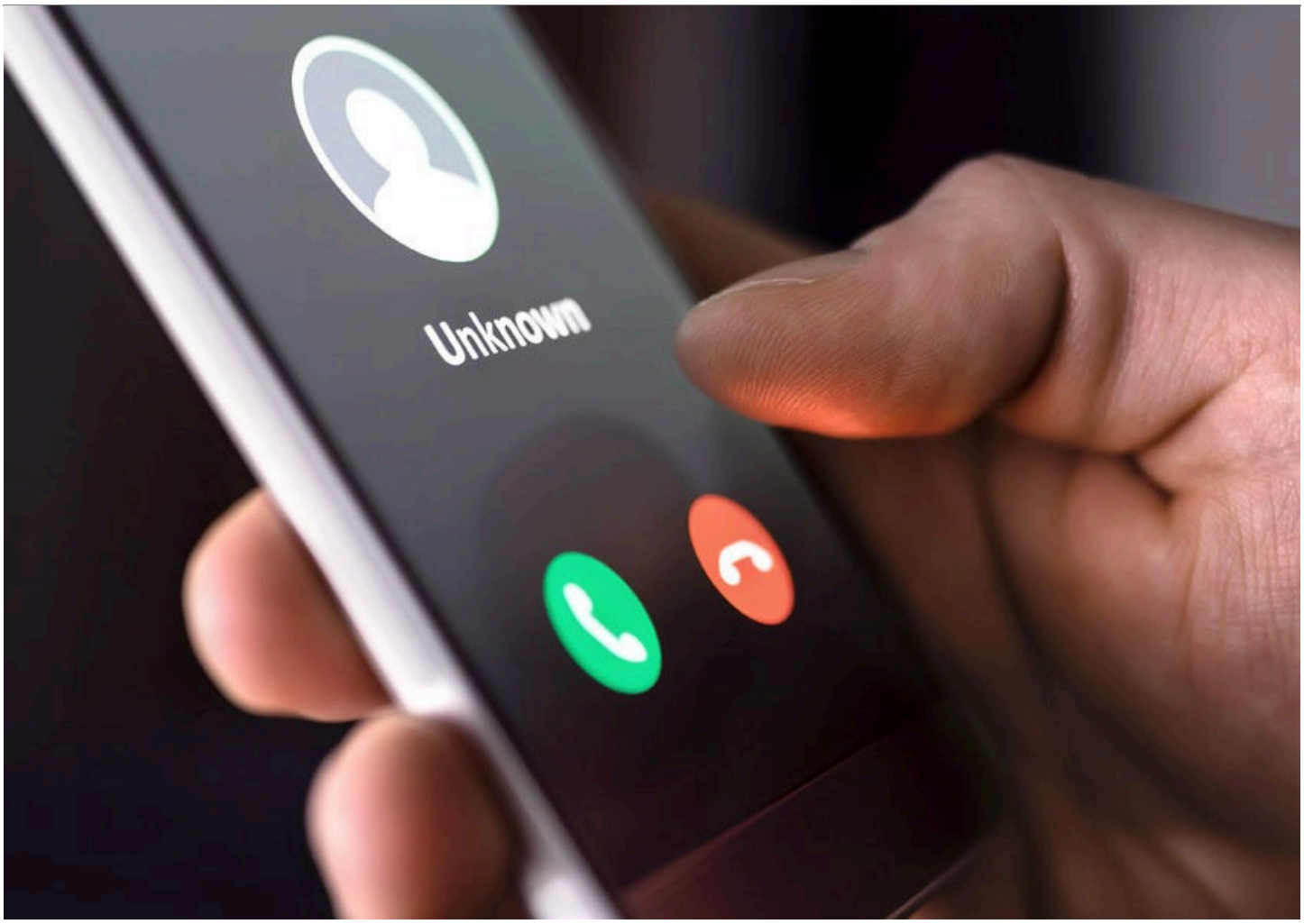
COVID-19 Scams Are on the Rise: Are You Protected?

Technology, Privacy, and eCommerce


Unknown



Online fraud is certainly not new, but they seem to have multiplied and spread as quickly as COVID-19. From Jan. 1, 2020 through Sept. 10, 2020, the US Federal Trade Commission has received nearly 200,000 consumer complaints, including more than 103,000 fraud reports, of which more than half include some level of financial loss, totaling over US$13 million so far.

This fraud does not appear to be isolated to any particular route. The full suite of standard tools is being leveraged from phishing emails and tests, to imposter schemes, social engineering, and robocalls. The new element is playing on the public panic and awareness of government assistance programs and economic worries.

How do scams impact corporations?

Because most people are working remote in our current working environment, individual threats are now corporate threats. Employees are cross-pollinating personal and work devices, which means that an employee who responds to a scam targeting them in a non-working role may wind up compromising work devices or information. Cybercriminals are banking on it.

As a concerned employer, companies should implement awareness programs for employees about scams — even those that are individual impact only — such as stock offers or personal financial scams. Individuals should be on high alert for scams, whether personal or work-related.

But the largest worry is phishing scams.

According to government sources, tens of thousands of domains have been purchased with keywords such as *vaccine or quarantine*. Individuals will receive an email from a supposedly legitimate organization, such as the World Health Organization, click on the link, and kick off a malware injection. Google reported in April that its Gmail platform blocked 18 million COVID phishing or malware emails a day along with over over 240 million COVID daily spam messages.

There are scams specifically targeting businesses, some with a variation of a known internal email directing employees to take actions like wiring funds (CEO scam) or downloading software (IT scam). These are particularly popular scams because companies are not in a “business as normal” mode. They are more susceptible to employees responding to an urgent message that meets a new business need, all in the midst of hectic home management. It’s a perfect storm for hackers.

Another popular phishing campaign is text messages that imitate a contact tracing app. Many individuals believe that tracing apps are pushed to their phones without their agreement, so they believe these alerts even if they have never installed one.

The damage that can result from a successful phishing campaign

Here are three examples of large companies that were targeted successfully by hackers:

- Facebook and Google were targeted by a Lithuanian group led by Evaldas Rimasauskas using fraudulent invoices for computer equipment that totaled over US$100 million.
- Crelan Bank in Belgium was a victim of the classic CEO scam and wired over US$75 million to the criminals, who have not been caught.
- The CEO scam also caught Aerospace Solutions of Austria for US$62 million.

These phishing attacks can be very sophisticated, targeting low level employees and then moving laterally and eventually vertically to target individuals with critical access. They may also target small businesses to build trust as vendors to larger corporations. They also spoof legitimate sites — according to Wandera’s 2020 Mobile threat Landscape report, there is a new phishing site every 20 seconds. That’s a lot of work aimed at your employees, data, and funds.

Steps to take to avoid scams

Many organizations report that they already engage in phishing education for employees. In this new environment with worries over disease and financials, working remotely, managing family in unusual routines, people are in a hurry and stressed.

However, education remains the best way to prevent phishing. People are the weakest link. Provide awareness of the seriousness of phishing both personally and to the company.

Use document preview for email attachments rather than downloading. This is available through several common corporate email providers.

Require multi-factor authentication. Yes, it is one more step, but it is a step that helps prevent compromised accounts.

Provide the appropriate resources to your IT and security departments. They need to run and maintain system health checks.

Educate employees about home network security. This doesn’t prevent phishing, but is a step to take to protect data.

Research security improvements. For example, Google states that no one participating in their Advanced Protection Program has been successfully phished, despite being repeatedly targeted.

In conclusion

As counsel, your role is to protect the company. If a phishing attack is successful, you may be involved with assessing the breach, recovering funds or data, working with authorities for resolution, or assisting the company in recovery. Thus, being aware of the risks and working with the right departments to prevent phishing may be a critical new element in your role to approach risk.

K Royal

Global Chief Privacy Officer

K Royal earned her JD from the Sandra Day O'Connor College of Law at Arizona State University. She also holds a PhD in Public Affairs from the University of Texas at Dallas.

Reach out to K about her column at @heartofprivacy on Twitter, or www.linkedin.com/in/kroyal/.