COVID-19
Best Fraud Prevention and Cybersecurity Practices

Payments Innovation Alliance®

August 2020

I. Increase security for online meetings

As social interaction increasingly shifts to Zoom and other video conferencing platforms, “Zoom bombing” has become a much-discussed form of disruption.[i] In an effort to curtail uninvited participants, these platforms have implemented measures such as requiring passwords upon joining meetings. Users can take additional steps to further ensure the integrity of their online meetings by designating co-hosts or moderators to monitor the chat room and step in, if necessary. Users can also take advantage of enhanced privacy features like a virtual “waiting room” that lets hosts see who is attempting to join prior to allowing access. Also, users are encouraged to generate random meeting links for extra privacy.

II. Be vigilant for potential malware

Hospitals and other institutions have come under ransomware attacks in light of the COVID-19 pandemic.[ii] To prevent ransomware, only download items from verified sources and never click unusual URLs or attachments. Furthermore, make it a habit to back up important data.

III. Increase awareness of potential phishing and scam emails

Coronavirus-themed phishing emails can come in different forms, but – as a general trend – claim to offer essential information or services.[iii] These can include variations of Centers for Disease Control and Prevention alerts, health advice emails, or workplace policy updates. Coronavirus themed emails that request personal information, have generic greetings, or spelling and grammar mistakes are often illegitimate in nature. The company should consider including headers or banners at the top of emails that mention the pandemic to heighten awareness. For example: “CAUTION: This email contains a reference to coronavirus or COVID-19.”

IV. Verify charities and other nonprofits before making donations

According to the Federal Trade Commission, there has been an increase in scams soliciting donations for fraudulent nonprofits and charities. The best way to curb this is by verifying the legitimacy of the nonprofit or charity through organizations such as the BBB Wise Giving Alliance or CharityWatch, which are both nonprofit and charity monitoring organizations.[iv] Fake organizations will not be able to verify their tax-exempt status nor be located on third-party websites, such as those maintained by the IRS or organizations that monitor and rank tax-exempt organizations. Fake organizations will often have generic greetings or grammatical errors in their communications.

V. Look out for scams related to government benefits

Scammers are using the pandemic as an excuse to target recipients of government benefits. According to the Social Security Administration, scammers have been calling benefit recipients and demanding social security numbers or banking information.[v] Similarly, scammers have attempted to take advantage of the recipients of stimulus checks from the CARES Act. In the case of both SSA benefits and stimulus checks, the government would not reach out to individuals for personal information.

VI. Use clear communications with customers

Scammers will tailor their scams to mimic actual communications from businesses to their customers about COVID-19 matters. Therefore, it is important for businesses and organizations, including financial institutions, to clearly communicate with their customers about new programs and promotions to help them differentiate from potential scams. For example, if insurance companies are providing rebate checks to customers, the company should inform recipients that a paper check will be sent and caution customers not to provide personal information in response to phishing emails that promise electronic deposits.

VII. Exercise caution with P2P payment services

Scammers are increasingly using person-to-person payment services to exploit people during the pandemic. For example, some scammers are offer "emergency funds" contingent on an initial payment or deposit for "verification purposes." [vi] Additionally, scammers often respond to comments or replies on official social media pages to lure in potential victims.

VIII. Take cybersecurity measures when working remotely

Experts recommend using a strong password for home Wi-Fi, avoiding public and unprotected networks, and using a virtual private network (VPN), which is a service that shields internet users by encrypting their data traffic. Use secure wireless connections for printers and wireless network expanders. Use only reputable mobile device scanning apps and avoid "easy" solutions, such as forwarding business documents to personal email accounts.

IX. Remember to exercise responsible management of hard copy documents

Employees may be printing more documents at home or using files and documents that are normally kept in an office. Remind employees to properly dispose of confidential documents, such as not throwing them in the household trash, for example. In addition, employees should exercise care if they are sharing a workspace with roommates or others who may inadvertently be exposed to confidential information.

X. Adapt your business resiliency plans to current situations related to COVID-19 [vii]

Update business resiliency plans to address operational challenges in a pandemic. This may include identifying critical functions and employees, and planning for how to work safely in the workplace or through remote working arrangements, if necessary. Companies should be prepared for an increase in information technology infrastructure usage and anticipate cybersecurity issues that may arise from remote working arrangements. Business resiliency plans should also take into account the ability of critical service providers and suppliers to continue operations during a pandemic.

Resources

Nacha:

- ACH Resources During the Coronavirus Pandemic: The Latest Information from Nacha on the ACH Network During the National Emergency
- Current Fraud Threats: Protect Your Organization From Fraud
- Protecting Against Fraud: How to Spot and Prevent Fraud Schemes

Other Resources:

- Consumer Financial Financial Protection Bureau: Helpful tips for using mobile payment services and avoiding risky mistakes
- Federal Trade Commission: Coronavirus Advice for Consumers
- The Cybersecurity and Infrastructure Security Agency: Defending Against COVID-19 Cyber Scams
- U.S. Securities and Exchange Commission: Look Out for Coronavirus-Related Investment Scams

This guidance was developed by the Cybersecurity Response Project Team of Nacha's Payments Innovation Alliance. This team develops tools and resources to help organizations understand evolving threats and identify questions and topics to address before, during and after a cyberattack. Previously, the team developed a template for organizations to use providing guidance and considerations in responding to security incidents. For more information about the Cybersecurity Response Project Team or to join, contact the Alliance at alliance@nacha.org or 703-561-1100.

About the Payments Innovation Alliance

The Payments Innovation Alliance is a 200-plus membership organization that brings together diverse, global stakeholders to support payments innovation. Through collaboration, discussion, debate, education, networking and special projects, the Alliance seeks to grow and advance payments and payments technology to better meet and serve the needs of the evolving industry. For more information and to learn how to join, visit **nacha.org/payments-innovation-alliance**.

About Nacha

Nacha is a nonprofit organization that convenes hundreds of diverse organizations to enhance and enable ACH payments and financial data exchange within the U.S. and across geographies. Through the development of rules, standards, governance, education, advocacy, and in support of innovation, Nacha's efforts benefit all stakeholders. Nacha is the steward of the ACH Network, a payment system that universally connects all U.S. bank accounts and facilitates the movement of money and information. In 2019, 24.7 billion payments and nearly $56 trillion in value moved across the ACH Network. Nacha also leads groups focused on API standardization and B2B payment enablement. Visit Nacha.org for more information, and connect with us on LinkedIn, Twitter, Facebook and YouTube.

[i] https://www.nytimes.com/2020/03/20/style/zoombombing-zoom-trolling.html

[ii] https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/coronavirus-used-in-spam-malware-file-names-and-malicious-domains

https://www.secureworldexpo.com/industry-news/how-will-ransomware-change-with-covid-19

[iii] https://us.norton.com/internetsecurity-online-scams-coronavirus-phishing-scams.html

https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/coronavirus-used-in-spam-malware-file-names-and-malicious-domains

[iv] https://www.consumer.ftc.gov/features/how-donate-wisely-and-avoid-charity-scams#research

[v] https://www.necn.com/news/coronavirus/scammers-are-trying-to-take-advantage-of-the-coronavirus-pandemic-nh-officials-warn/2259807/

[vi] https://qz.com/1827085/cash-app-scammers-are-using-coronavirus-to-exploit-people/

[vii] https://www.ffiec.gov/press/pr030620.htm

Payments
Innovation Alliance®