The Surety & Fidelity Association of America
Serving the Industry Since 1908

SFAA BULLETIN

INCREASES IN COMPUTER HACKING AND SOCIAL ENGINEERING FRAUD EXPOSURE RESULTING FROM MOVE TO REMOTE WORKING ENVIRONMENT:

As a result of the COVID-19 pandemic and the shelter in place orders issued by state governments, all non-essential businesses have shifted to remote working from home to maintain their business operations. As a consequence, the FBI warned that this practice is presenting a growing security threat to businesses as cyber criminals look to exploit telework software vulnerabilities in order to obtain sensitive information, eavesdrop on conference calls or virtual meetings, or conduct other malicious activities. We present this information to you so that you can better assess the risks you are underwriting and to help you educate your Insureds. The SFAA continues to monitor developing fraud exposures and will provide additional updates as warranted.

1. TELEWORK VULNERABILITIES:

The FBI recommends businesses carefully consider the software the organization uses for telework applications, including video conferencing software and voice over Internet Protocol (VOIP) conference call systems. Users should consider the risks associated with them and apply cyber best practices to protect critical information, safeguard user privacy, and prevent eavesdropping.

The FBI has provided the following list of methods cyber criminals may use to exploit telework applications.

A. Software from Untrusted Sources

- Cyber Fraudsters may offer free or reduced cost telework software that otherwise looks legitimate, to gain access to sensitive data or eavesdrop on conversations.
- Cyber Fraudsters may also use phishing links or malicious mobile applications that appear to come from legitimate telework software vendors.

B. Communication Tools

- Malicious cyber actors may target communication tools (VOIP phones, video conferencing equipment, and cloud-based communications systems) to overload services and take them offline or to eavesdrop on conference calls.
- Cyber actors have also used video-teleconferencing (VTC) hijacking to disrupt conferences by inserting pornographic images, hate images, or threatening language.

C. Remote Desktop Access

- Cyber Fraudsters have targeted remote desktop sharing applications to compromise these systems and to gain access to other shared applications.

D. Supply Chain

- Some organizations looking to obtain computer equipment to enable teleworking are renting equipment from foreign sources. The FBI warns that any previously used equipment that has not had its hard drive wiped of all information prior to use could potentially carry preinstalled malware.

Teleworking Tips to Protect the Organization:

The FBI published the following recommendations to protect businesses from fraud relating to the software utilized for teleworking platforms.

- Select trusted and reputable telework software vendors; conduct additional due diligence when selecting foreign-sourced vendors.
- Restrict access to remote meetings, conference calls, or virtual classrooms, including the use of passwords, if possible.
- Beware of advertisements or emails purporting to be from telework software vendors.
- Limit access to teleworking functions like Remote Desktop Protocol (RDP) or Virtual Network Computing (VCN) to only required individuals.
- Do not share links to remote meetings, conference calls, or virtual classrooms on open websites or open social media profiles.
- Never open attachments or click links within emails from senders you do not recognize.

2. SOCIAL ENGINEERING FRAUD (SEF)

The FBI is advising that over the past several weeks SEF fraudsters have impersonated vendors and asked for payment outside the normal course of business due to COVID-19. The FBI advises that every organization should establish the following fraud prevention policies and procedures:

- Procedures to verify any changes to customer or vendor details, independent of the requester of the change. Examples of these procedures would include:
  - Direct call back to the customer or vendor using only the telephone number provided by customer or vendor prior to request being made.
  - Confirmation of change request is made with someone at the customer or vendor level, other than the individual who requested the change.
  - Sending a verification text message to a predetermined number.
  - Receipt by the company of a code known only to the customer to determine identity.
- Procedures to verify last-minute changes in wiring instructions or recipient account information.
  - Use call-back procedures to clients and vendors for all outgoing fund transfers to a previously established phone number or implement a verification system with similar dual verification properties.
  - Verify vendor information via the recipient's contact information on file—do not contact the vendor through the number provided in the email.
- Verify the email address used to send emails, especially when using a mobile or handheld device, by ensuring the sender's email address appears to match who it is coming from.
  - Check the email address by hovering your mouse over the 'from' address. Make sure no alterations (like additional numbers or letters) have been made.

1140 19TH STREET NW, SUITE 500, WASHINGTON, DC 20036 • TEL: (202) 463-0600 FAX: (202) 463-0606
WWW.SURETY.ORG • INFORMATION@SURETY.ORG

- If you discover you are the victim of a fraudulent incident:
  - Immediately contact your financial institution to request a recall of funds.
  - Contact your employer to report irregularities with payroll deposits.
  - As soon as possible, file a complaint with the FBI's Internet Crime Complaint Center at BEC.IC3.gov.

3. OTHER CYBER FRAUD PREVENTION RECOMMENDATIONS:

The FBI has provided the following additional tips that can help protect individuals and businesses from being victimized by Cyber Fraudsters:

- Verify the web address of legitimate websites and manually type them into your browser.
- Change passwords for routers and smart devices from default setting to unique passwords.
- Check for misspelled domain names within a link (for example, confirm that addresses for government websites end in .gov).
- Report suspicious activity on work computers to your employer.
- Use multi-factor authentication (MFA) when accessing organizational sites, resources, and files.
- Practice good cyber security when accessing Wi-Fi networks, including use of strong passwords and Wi-Fi Protected Access (WPA) or WPA2 protocols.
- Ensure desktops, laptops, and mobile devices have anti-virus software installed and routine security updates are applied; this includes regularly updating web browsers, browser plugins, and document readers.
- Beware of social engineering tactics aimed at revealing sensitive information. Make use of tools that block suspected phishing emails or allow users to report and quarantine them.
- Do not open attachments or click links within emails received from senders you do not recognize.
- Do Not provide usernames, passwords, birth dates, social security numbers, financial data, or other personal information in response to an email or phone call.
- Never use public or non-secure Wi-Fi access points to access sensitive information.
- Avoid using the same password for multiple accounts.

1140 19TH STREET NW, SUITE 500, WASHINGTON, DC 20036 • TEL: (202) 463-0600 FAX: (202) 463-0606
WWW.SURETY.ORG • INFORMATION@SURETY.ORG

ADDITIONAL SOURCES OF INFORMATION RELATING TO COVID-19 CYBER RISKS

The following is a list of additional sources for information relating to emerging COVID-19 Fraud exposures.

FBI:

- FBI resources relating to Covid-19 related fraud:
  - **www.FBI.gov**
  - **www.fbi.gov/coronavirus**
  - **www.ic3.gov**
  - National Cyber Investigative Joint Task Force (NCIJTF) **www.fbi.gov/investigate/cyber/national-cyber-investigative-joint-task-force**

US Department of Justice:

- US Department of Justice Combating Corona Virus Fraud Page **www.justice.gov/coronavirus**

Federal Trade Commission:

- FTC resources relating to Covid-19 related fraud: **www.FTC.gov**
  - The FTC's free online security tips and resources, and share with your friends, family, coworkers, and community. **https://www.consumer.ftc.gov/features/feature-0038-onguardonline**
  - "Is that text message about your FedEx package really a scam?" **https://www.consumer.ftc.gov/blog/2020/02/text-message-about-your-fedex-package-really-scam**
  - "While you're at home, spot the scams." **https://www.consumer.ftc.gov/blog/2020/04/while-youre-home-spot-scams**

Cybersecurity and Infrastructure Security Agency (CISA) (www.cisa.gov):

- National Cyber Awareness System:
  The National Cyber Awareness System offers a variety of information including Alerts, Analysis Reports, Current Activity, or Bulletins for users with varied levels of technical IT expertise.
  https://www.us-cert.gov/ncas

U.S. Department of Health and Human Services (HHS):

- HHS COVID-19 Fraud Alert:
  https://oig.hhs.gov/coronavirus/fraud-alert-covid19.asp?utm_source=web&utm_medium=web&utm_campaign=covid19-fraud-alert

Federal Communications Commission (FCC):

- FCC Scam Glossary:
  https://www.fcc.gov/scam-glossary

1140 19TH STREET NW, SUITE 500, WASHINGTON, DC 20036 • TEL: (202) 463-0600 FAX: (202) 463-0606
WWW.SURETY.ORG • INFORMATION@SURETY.ORG

FINRA:

- FINRA guidance, updates and other information to help stakeholders stay informed about the latest developments.
  https://www.finra.org/rules-guidance/key-topics/covid-19?utm_source=Nasdaq&utm_medium=Coronavirus_501&utm_campaign=Syndication

Securities and Exchange Commission (SEC):

- SEC updated information on its response to COVID-19 and the related effects on our securities markets.
  https://www.sec.gov/sec-coronavirus-covid-19-response

Commodities Futures Trade Commission (CFTC):

- The Commodity Futures Trading Commission dedicated website to highlight the Commission's actions related to COVID-19
  https://www.cftc.gov/coronavirus

The Better Business Bureau (BBB):

- BBB updated COVID-19 scam alerts:
  https://www.bbb.org/council/coronavirus/

1140 19TH STREET NW, SUITE 500, WASHINGTON, DC 20036 • TEL: (202) 463-0600 FAX: (202) 463-0606
WWW.SURETY.ORG • INFORMATION@SURETY.ORG