Texas Council
Risk Management Fund

CYBER SECURITY DURING A PANDEMIC – REMINDERS AND WHERE TO REPORT A CYBER INCIDENT

For many organizations, the increased dependency on technology and virtual environments as a result of the pandemic have created a breeding ground for cyber criminals. According to the *European Journal of Information Systems, Volume 29, 2020 – Issue 3: Business Process Management and Digital Innovation*, cybercrimes are escalating dramatically, and more alarming are the high volumes of COVID-19 themed scams. Phishing and hacking attacks and threats have increased by 5 to 6 times their usual numbers in the month of March and more than 42,000 websites with domains containing "COVID" and "Corona" have been registered – the majority of these appear to be suspicious (Kumaran & Lugani, 2020). In April, the FBI's Internet Crime Complaint Centre received between 3,000 and 4,000 cybersecurity complaints daily compared to an average 1,000 daily complaints before COVID-19 (Cimpanu, 2020). Not surprisingly, Web credit card skimming increased by 26 percent in March due to the recent growth in online shopping (Segura, 2020).

It is important to remain diligent and aware of the vulnerabilities we face while online. Below are few reminders and best practices to implement in your daily work.

1. Be very suspicious of interactive dashboards reporting COVID-19 infections and death rates. These are being used in malicious websites and emails to spread password-stealing malware. Criminals have also started selling COVID-19 infection kits for deployment of malware.
2. Be aware of an increase in phishing attacks that use a combination of email and fake websites to trick users into revealing sensitive information. Never reveal personal information or financial information including your name or address.
3. Be cautious of disinformation campaigns that spread discord, manipulate public conversation, influence policy development, and disrupt markets.
4. Use extreme caution. Avoid clicking on links in unsolicited emails and be wary of email attachments. Cyber criminals have started sending email scams that prey on a person's desire to help during the Coronavirus crisis. These malicious emails inform the recipient to open an attached document that includes information about safety measures which then directs users to a page that asks for their email address and password. Any grammatical errors in the email address or message may be indicative of a potential cyber-attack.
5. Use only official state agency websites and social media accounts such as: Public Health, Governor's Office, Homeland Security and Emergency Management, Attorney General, and Centers for Disease Control.

6. Verify a charity's authenticity before making donations. Review the Federal Trade Commission's blogs for current information on avoiding COVID-19 related scams at: www.consumer.ftc.gov/blog/2020/02/coronavirus-scammers-follow-headlines
7. Update Virtual Private Networks (VPNs), network infrastructure devices, wireless devices, and devices being used to remotely connect to work environments with the latest operating systems, software patches and security configurations. Unpatched network infrastructure equipment, servers and end user equipment continue to be an attractive target for malicious actors.
8. If a VPN is not implemented, require all users, especially remote users, to use very strong passwords. A minimum length of 16 characters containing numbers, symbols, upper/lower case letters, and spaces is recommended. Attackers can steal a weak password using dictionary attacks and automated tools.
9. Avoid using Remote Desktop Protocol (RDP), if possible. This protocol connects a user to another computer remotely over a network connection. This leaves RDP client ports open to the Internet, leaving vulnerability to attackers that scan blocks of IP addresses for open RDP ports.
10. Enhance system monitoring to receive early detection and alerts on abnormal activity. Ramp up remote access log review and attack detection.
11. Ensure all machines and wireless devices have properly configured network firewalls as well as anti-malware and intrusion prevention software installed. Most operating systems include a built-in firewall feature to enable for added protection.

For members of the Fund that have elected to purchase Cyber coverage with Beazley, cyber incidents including compromised email, ransomware, release of W-2 to an outside party, unauthorized access to Office 365 accounts, and wire transfer fraud, should be reported to the Fund and Beazley. To do so, send an email to bbr.claims@beazely.com with the following:

- Name of your center and insurance policy number. *If you do not have your policy number or you're unclear if your center has this coverage, please contact the Fund.*
- A short description of the incident
- Date the incident occurred (if known)
- Date you discovered the incident
- Contact information for the point person handling the investigation at center
- Copy your senior Customer Service Representative at the Fund on this email
- Do not include any personally identifiable information or protected health information
- Use the word "incident" and not "breach" in your notice

For additional information regarding cyber coverage or reporting procedures, please contact the Fund.

Kumaran, N. , & Lugani, S. (2020) *Identity and security. Protecting businesses against cyber threats during COVID-19 and beyond* . Retrieved 24 August,020 from https://cloud.google.com/blog/products/identity-security/protecting-against-cyber-threats-during-covid-19-and-beyond

Cimpanu, C. (2020) *FBI says cybercrime reports quadrupled during COVID-19 pandemic* . Retrieved 24 August, 2020 from https://www.zdnet.com/article/fbi-says-cybercrime-reports-quadrupled-during-covid-19-pandemic/

Segura, J. (2020) *Online credit card skimming increased by 26 percent in March.* Accessed 24 August 2020 from https://blog.malwarebytes.com/cybercrime/2020/04/online-credit-card-skimming-increases-by-26-in-march/