Charles G. Cooper
Commissioner

TEXAS DEPARTMENT OF BANKING

2601 North Lamar Blvd., Austin, Texas 78705
512-475-1300 /877-276-5554
www.dob.texas.gov

Media Contact:
media@dob.texas.gov

INDUSTRY NOTICE 2020-07
Date: April 8, 2020

Increased Cyber Activity During Times of Crisis

During times of crisis, cybercriminals and nation-state actors often exploit financial institutions and their customers for financial or political gain. For this reason, the Department of Banking in conjunction with the Independent Bankers Association of Texas and the Texas Bankers Association developed a list of areas that you, your staff, and your customers should consider.

Evaluating cybersecurity readiness can be accomplished by utilizing the PPT model that considers: **People, Processes, and Technology.**

I. People

- Continue to remind your employees that human error as a result of social engineering schemes, rather than the use of sophisticated technologies, remains the top method of cyber attacks. Emphasize key training lessons and regularly remind employees to stay vigilant.
- Let remote workers know when online/virtual meeting platform links are expected and legitimate. If something does not look right, employees should contact the meeting organizer.
- Remind customers and staff that some banks/branches may have adjusted hours or services in compliance with Centers for Disease Control (CDC) guidance, but customers continue to have access to funds and deposits remain FDIC-insured and safe.
- Inform customers and employees that your institution's brand might be used in a fraudulent alert to customers. These fraudulent alerts may state that the customer's bank account has been temporarily suspended. The victim may receive a link that looks like your bank's login screen, encouraging them to log in with their banking username and password.
- Communicate to customers that dis-information campaigns are already underway and to only rely on government and well-established news sources for credible information such as the CDC, the World Health Organization (WHO), and the Department of Homeland Security. Be wary of unreliable websites and random social media posts.
- Inform customers and staff that scams are preying on fear and interest in COVID-19. They should be extra cautious about clicking links and providing sensitive or confidential information. Be extra vigilant to follow secure cyber practices:

- Do not click on attachments or links from individuals or organizations that you are not expecting or from someone you do not know.
- Pay close attention to email and web addresses. Look for misspellings, grammar mistakes or other red flags.
- Hover the mouse cursor over hyperlinks to see where they lead.
- Avoid messages that urge you to *act now*. This sense of urgency is meant to pressure people into making irrational decisions.

- Remind your staff and customers to be cautious of communications with the following or similar subjects:
  - Obtaining U.S. government funding related to Coronavirus relief.
  - Check for an updated Coronavirus map in your city.
  - Coronavirus infection warnings from local school districts/governmental entities.
  - Keep your children safe from Coronavirus.
  - Raise funds for Coronavirus victims – (If you wish to donate money, consider only working with known and established organizations and donate through their official websites or phone numbers. Avoid responding directly to email solicitations.)

II. Processes

- Re-distribute your Information Technology (IT) policy to employees. A reminder about expectations for acceptable/required behaviors is important.
- Anticipate Distributed Denial of Service (DDoS) attacks are often distractions to carry out wire fraud.
- Exercise special caution when honoring customer requests for special/alternative handling of transactions. Requests for wire transfers or ACH account changes should be verified by contacting the business contact on a known phone number, asking a fellow staff member to review the requests, or calling the customer directly.
- Be vigilant against Business Email Compromise (BEC). Attacks typically consist of an email in which an institution executive is impersonated (spoofed) and asks an employee to wire funds to an outside account. Bank policies should be in place to require secondary confirmation of major wires or transactions in-person or by telephone.
- Look out for Corporate Account Takeover (CATO) attempts. The attacks are usually in the form of emails that ask for your credentials. Ensure that bank IT policies contain instructions to contact your IT or Security team before releasing information if a password is requested by email.
- Review your cyber incident response plan. Roles and responsibilities among executives should be clear. Staff should know what they should do and who to contact during an incident/event.
- Be Mindful of Incident Notification Requirements. Under Title 7, Texas Administrative Code §3.24, the Texas Department of Banking requires a state bank to notify the banking commissioner promptly when a material cybersecurity incident occurs whether systems are maintained by the bank or by an affiliate or third-party service provider.

III. Technology

- As you utilize alternative systems/equipment in conjunction with your Business Continuity Plan, remember to follow your standard security protocol.
- Maintain Secure Connections for Remote Workers.
    - Can you assist staff in securing their home Wi-Fi? Remind staff that public Wi-Fi networks should be avoided.
    - If use of personally owned devices for remote access is allowed, help staff bring these devices up to date with the latest security patches and end-point protection.
    - Implement multi-factor authentication for high-risk remote access.
    - Discuss with your managed service provider (MSP) how they are maintaining security to your network with any of their remote workers.

Other Important Considerations

- **Cyber Insurance**
    - Know what your policy(s) covers (e.g. forensic remediation, notification expenses, equipment replacement, reputation repair, etc.).
    - Understand your policy's exclusions and how the insurer defines "minimum security standards."
    - Confirm that required security protocols are in place including when employees are working from home.