Individual Advice for Customers and Employees to Protect Financial Data

Advise your employees and your customers to follow the below cybersecurity guidelines in their personal behavior to increase their preparedness and protect their financial data against cyber threats.

1. Implement basic cyber hygiene practices across your devices.
   - Use strong passwords on all personal and professional devices, and consider using a password manager.
   - Keep operating systems and other software and applications up to date on your computers and mobile devices.
   - Install anti-virus, anti-malware, and anti-ransomware software that prevents, detects, and removes malicious programs.
   - Use a firewall program to prevent unauthorized access to your computer.
   - Only use security products from reputable companies. Read reviews from computer and consumer publications and consider consulting with the manufacturer of your computer or operating system.

2. Be careful with sensitive information.
   - Do not send bank account passwords or other sensitive financial account data over unencrypted email.
   - Be smart about where and how you connect to the Internet for banking or other communications involving sensitive personal information. Public Wi-Fi networks and computers at places such as libraries or hotel business centers can be risky.

3. Resist phishing.
   - Don’t immediately open email attachments or click on links in unsolicited or suspicious-looking emails. Stop. Think. Click.
   - Be suspicious if someone contacts you unexpectedly online or via telephone and asks for your personal information. Even when communicating with known addresses, minimize sharing of personal information via email.
   - Remember that no financial institution will email or call you and request confidential information they already have about you.
   - Assume that a request for information from a bank where you have never opened an account is a scam.
   - Verify the validity of a suspicious looking email or a pop-up box before providing personal information. Pay close attention to the email address.
TRAINING EMPLOYEES

• Teach your employees accountability and strategies to minimize human error that could expose customer data. This means advising them to:
  • Minimize their access to and transmission of customer data to only what is necessary to perform their job functions,
  • Maintain strong security practices on all devices and accounts that deal with customer data by using strong passwords, enabling two-factor authentication, keeping software updated, and not clicking on suspicious links, and
  • Report any potential internal or external security incidents, threats, or mishandling of data to your organization’s technical personnel and/or higher management.
• Ensure your employees understand and have signed documents to adhere to your organization’s data protection and security policies so that they do not violate them, so they are fluent when dealing with customers, and so they do not communicate with customers in an unprotected manner.

NOTIFYING CUSTOMERS

• Understand your organization’s regulatory environment when it comes to handling customer data breaches to ensure you are prepared to comply when incidents do occur.
• When your organization becomes aware of an incident of unauthorized access to sensitive customer information, investigate to promptly determine the likelihood that the information has been or will be misused. Follow notification best practices and notify the affected customer(s) accordingly as soon as possible with:
  • A general description of the incident and the information that was breached,
  • A telephone number for further information and assistance,
  • A reminder “to remain vigilant” over the next 12 to 24 months,
  • A recommendation that incidents of suspected identity theft be reported promptly,
  • A general description of the steps taken by the financial institution to protect the information from further unauthorized access or use,
  • Contact information for credit reporting agencies, and
  • Any other information that is required by regulations with which your organization must comply.