Fidelity Bank
Helping you get where you want to be℠

LifeDesign Banking®

Information Security Best Practices

A Guide for Reducing the Risk of Data Breach and Fraud

INTRODUCTION

Fidelity Bank is committed to providing our clients with a safe and secure online operating environment. Sometimes even with the best security in place bad things can happen. Over the past few years cyber criminals have significantly increased their level of activity and their level of sophistication in order to attack banks and their clients. We have put together the following security guidelines to help our clients decrease their chances of falling victim to cyberattacks.

These guidelines expand upon a three-part risk management framework developed by the United States Secret Service, the Federal Bureau of Investigation, the Internet Crime Complaint Center (IC3), and the Financial Services - Information Sharing and Analysis Center (FS-ISAC). Fundamentally, best practices for managing information security risks in terms of processes and controls center the following core elements:

- **Protect**
- **Detect**
- **Respond**

The following best practices have been compiled for each of the recommended processes and controls under the Protect, Detect, and Respond framework. These best practices are not an all-inclusive list and are provided as guidance to assist in implementing processes and controls needed to reduce the risk of identity theft and fraud.

Cybercrime is a Significant Threat

- Criminals target victims by various online scams such as sending malicious email attachments or malicious websites (including Social Networking sites).
- Victims unknowingly install malicious software by clicking on a link embedded in an email or visiting an infected Internet site.
- It is important to remember that electronic crimes are dynamic as cyber-criminals continually change their techniques. Additional changes in risk management processes and controls will be necessary as this type of theft continues to evolve.

Key Steps to Protect Your Data and Systems – This Applies to Systems Used to Perform Financial Transactions in Particular

1. Stealing or hacking passwords has become one of the most pervasive cybersecurity threats. If possible, consider utilizing multifactor authentication (MFA) for all critical business systems – including email. If MFA is not feasible you should ensure that you are using the strongest passwords possible and that your employees under stand the importance of keeping their passwords safe and secure.
2. Ensure that your employees are well trained on security best practices. Email phishing and credential stealing are huge threats to security. Your employees should be trained on how to recognize and react to these types of attacks. This type of training should be performed on a regular basis.
3. Install and maintain real-time anti-virus, desktop firewall, and malware detection and removal programs; Use these tools regularly to scan your computers. Allow for automatic updates and scheduled scans.
4. Utilize Internet content filtering systems that will prevent employees from accessing known dangerous web sites.
5. Install and maintain Spam Filters.
6. Firewalls should be used and the rules should only allow services that are required for conducting business. Change the default passwords for your firewalls.
7. Promptly install all available security updates on all systems, especially those systems used to facilitate financial transactions.
8. Adopt advanced security measures by working with security consultants or dedicated IT staff.
9. Periodically review employee access rights to internal and online systems, make sure access levels are appropriate for job responsibilities.
10. Remove employee access promptly upon termination.
11. It is highly recommended that users do not have administrative rights on their work computers to prevent unauthorized software from being downloaded (business owners should discuss this with their IT departments or service providers).
12. Utilize resources provided by trade organizations and agencies that specialize in helping small businesses.
13. Implement procedures to alert us if you suspect a problem.
14. Subscribe to security education resources (See Appendix A).

It is highly recommend that you consider the following with regards to systems used to perform financial transactions:

1. It is highly recommended that a dual control process is implemented, which requires one employee to setup a transaction and another to approve the transaction. If you have any questions about this type of control we will be happy to discuss this with you.
2. Consider using a dedicated PC that is used exclusively for performing financial transactions. This PC should NOT be used for send or receive email or browse the Internet.

Detect Issues Before They Become Serious

Detection is closely associated with protection, as some measures to protect against electronic theft will also be an indication that a theft is being attempted. You should be alert for some red flags related to computer and network anomalies:

1. Passwords no longer work.
2. Unexplained requests for passwords or requests asking to reset passwords.
3. Unexpected requests to re-login to systems that you are already logged in to.
4. Unexplained inability to log into online banking system.
5. Sudden changes in the way web pages, graphics, text or icons appear.
6. Unexpected rebooting or restarting of a computer.
7. Unexpected requests for one-time passwords (or tokens) in the middle of an online session.
8. Unusual pop-up messages, especially a message in the middle of a session that says the connection to the institution's system is not working (system unavailable, down for maintenance, etc.); "try back later" or "system is undergoing maintenance".
9. New or unexpected toolbars and/or icons.
10. It is VERY important to ensure that system and operating system logs are configured to capture critical security information. Monitoring these logs may prevent an issue from occurring and will help to determine what actually happened when or if an event does occur.

Respond

1. You should immediately contact us if you suspect that online banking credentials have been compromised.
2. Consider that your email may have also been taken over and may not be a secure method of communicating information. Calling us is the best way to communicate that there may be an issue.
3. Contact your IT Department or service provider and report the issue to them as soon as possible.

APPENDIX A

Information Security Resources

1. The Federal Communications Commission (FCC) Cybersecurity Planning Guide:

   https://www.fcc.gov/cyberplanner

2. The Federal Trade Commission's (FTC) guide for online security:

   https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business

3. USCERT Cybersecurity Resources for small to medium size businesses:

   https://www.us-cert.gov/ccubedvp/smb

APPENDIX B

Be Aware

1. Fidelity Bank will never directly contact you via email to install software upgrades. Such messages should be treated as fraudulent and you should permanently delete these messages and not click on any links.
2. Messages or inquiries from the Internal Revenue Service, Better Business Bureau, FDIC, and almost any other organization asking you to install software, provide account information or access credentials is most likely fraudulent.
3. Phone calls and text messages requesting sensitive information are likely fraudulent. If in doubt, you should contact the organization at the phone number that you obtained from a reliable source. You should not call phone numbers (even with local prefixes) that are listed in the suspicious email or text message.

APPENDIX C

Incident Response Plan

Since each business is unique, you should write your own incident response plan. A general template would include:

1. IT Department / service provider contact numbers;
2. Fidelity Bank contact numbers: Cash Management Operations 978-870-1472
   Client Care Center 978-870-1400 or 800-581-5363
3. Limit further unauthorized transactions:
   a. Change user and administrative passwords;
   b. Disconnect computers used for Internet banking;
   c. Request a temporary hold on all transactions until out-of-band confirmations can be made;
4. Contact your insurance carrier;
5. Work with your IT Department, service provider, and dedicated information security specialists (preferred) to review your systems; and
6. Contact law enforcement if you suspect a crime has been committed.