Security Considerations for Businesses

In accordance with Federal Regulatory guidelines and sound business practices, Central Penn Bank has implemented a security program to specifically address identified risks in offering internet-based services to its customers. The bank recognizes that the most sophisticated and expensive security program can be rendered ineffective if combined with the absence of fundamental customer controls. Thus, we need you to consider the following guidelines for your business so that together we can maintain a safe environment for conducting business transactions online.

Risk Assessment - What If?

Central Penn Bank has created an extensive list of "What If" scenarios to consider that present varying degrees of risk to the bank and its ability to continue conducting business. These risks are categorized into technical risks including internet related, computer and telecommunications; human risks such as fraud, error and robbery; and natural risks including flooding, fire and snow. A response plan has been created to respond to each risk. We suggest that you also consider doing this for your business.

To address specific risks from conducting business online, consider the following questions:

- Do you have a password policy that requires the use of strong passwords (includes at least 3 of the following elements, upper case letter, lower case letter, number or special character?)
- What is your password lockout policy?
- How frequently are passwords required to be changed?
- Are passwords being written somewhere such as on the back of the monitor or underside of a keyboard by employees?
- Can passwords previously used be repeated? Is this based on number of days since last use or the number of times since last use?
- Does your company conduct background checks on employees? The cost is minimal compared to the potential loss from fraud.
- Are computer system rights and permissions revoked in a timely manner for dismissed employees? Does this include all remote devices?
- Are duties segregated sufficiently to create effective checks and balances if possible?
- Do you have a data backup? Is this tested periodically? If this data is transported to another location, is it encrypted or have password protection to guard sensitive data?
- Does your business have insurance coverage for losses resulting from these events? Do you understand what is not covered?
- Have you considered reconciling or reviewing account activity daily?
- Do you ensure that PC and network related patches and components are up-to-date?
- Do you ensure that anti-virus and anti-malware software programs are up-to-date?
- Do you provide periodic communication and training to employees using online banking systems?
- Are dual controls in place where applicable, i.e. to originate and transmit ACH files?
- Consider using dedicated IT staff or a consultant to implement security measures.

Utilize resources provided by trade organizations and agencies who specialize in helping small businesses. These include:

- The Better Business Bureau
- The Small Business Administration (SBA)
- The Federal Trade Commission's (FTC)
- The National Institute of Standards and Technology (NIST)
- Review and/or consider insurance coverage to cover incidents relating to electronic theft.

Internet Usage / Email Policy

If your business does not have a policy on internet usage for your employees, please consider adopting one. Though the web can be an incredibly useful workplace tool, it can also cause significant workplace havoc that can result in lost productivity, financial loss, liability and damage to the reputation of your business. Unscrupulous websites, as well as pop-ups and animations, can be dangerous. Establish rules about internet usage including email guidelines to protect your business — and your employees.

Why Your Business is at Risk

Web pages contain programs that are usually innocent and sometimes helpful - for instance, animations and pop-up menus. However, there are questionable, even malicious web sites that have their own agenda, and it is not always in your best interests. When surfing the web, site operators can identify your computer on the internet, tell which page you came from, use cookies to profile you and install spyware on your computer - all without your knowledge. Destructive worms can also enter your system through your web browser.
Beyond malicious activities instigated by outsiders, employees who engage in illegal and/or undesirable web activity during work hours and on company-owned computers can put businesses in a vulnerable position.

What Your Internet Policy Should Include

When creating a company-wide internet use policy, consider addressing the following issues:

- Are employees allowed to browse the web for personal use as well as business purposes?
- Can employees use the web for personal use (lunch hours, after-hours, etc.?)
- Does the company monitor web use? What level of privacy can employees expect?
- Is certain web activity prohibited? Spell out unacceptable behavior in detail. In many companies, this includes:
  - Downloading offensive content
  - Threatening or violent behavior
  - Illegal activities
  - Commercial solicitations (non-business related)

Provide two copies of the policy to employees. One for them to keep and another for them to sign and return to you. The signed copy provides written proof that the employee was made aware of company policies, possible consequences of violating company policies and that they understand and accept these conditions.

Tips for Safe Browsing

In addition to having a policy, the following recommendations can also help promote safe web browsing:

- Go to trusted sites only.
- Do not use work computers for idle browsing.
- Never browse web sites from a server – always use a client PC or laptop.
- Use a firewall/router – it allows you to filter web addresses and block internet traffic to and from dangerous sites.
- Consider web-filtering software.
- Develop an incident response plan to address security breaches.

Warning Signs of Potentially Compromised Computer Systems

- Inability to log into online banking (Thieves could be blocking customer access, so the customer will not see the theft until the criminals have control of the money.)
- Dramatic loss of computer speed
- Changes in the way things appear on the screen
- Computer locks up so the user is unable to perform any functions
- Unexpected rebooting or restarting of the computer
- Unexpected request for a one time password (or token) in the middle of an online session
- Unusual pop-up messages, especially a message in the middle of a session that says the connection to the bank system is not working (system unavailable, down for maintenance, etc.)
- New or unexpected toolbars and/or icons
- Inability to shut down or restart the computer

Additional Security Measures

Examples of deceptive ways criminals contact account holders:

- The FDIC does not directly contact bank customers (especially related to ACH and Wire transactions, account suspension, or security alerts), nor does the FDIC request bank customers to install software upgrades. Such messages should be treated as fraudulent and the account holder should permanently delete them and not click on any links.
- Messages or inquiries from the Internal Revenue Service, Better Business Bureau, NACHA, and almost any other organization asking the customer to install software, provide account information or access credentials is probably fraudulent and should be verified before any files are opened, software is installed or information is provided.
- Phone calls and text messages requesting sensitive information are likely fraudulent. If in doubt, account holders should contact the organization at the phone number the customer obtained from a different source (such as the number they have on file, that is on their most recent statement or that is from the organization's website). Account holders should not call phone numbers (even with local prefixes) that are listed in the suspicious email or text message.

Applicable Laws & Regulations

It is important that businesses understand that a breach of customer information can potentially create financial and reputational risks for the business. For certain businesses, or those utilizing certain services such a debit and credit cards payments, compliance with applicable rules to secure data is necessary to prevent potential lawsuits, cancelled accounts and monetary fines.
Please be aware that banking regulations regarding liability differ between consumer accounts and business/corporate accounts. Please contact us with any questions you may have.

Incident Response Plan

If you suspect that your computer system has been compromised, having an action plan to follow can save time critical to preventing loss. Consider developing a plan that includes the following information and action steps:

- Contact information for key financial institution employees
- Changing passwords
- Disconnecting computers used for internet banking
- Requesting a temporary hold on all other transactions until out-of-band confirmations can be made
- Insurance carrier contact information
- Working with forensic specialists and law enforcement to review appropriate equipment