Is your company keeping information secure?

Are you taking steps to protect personal information? Safeguarding sensitive data in your files and on your computers is just plain good business. After all, if that information falls into the wrong hands, it can lead to fraud or identity theft. A sound data security plan is built on five key principles:

1. **Take stock.** Know what personal information you have in your files and on your computers.
2. **Scale down.** Keep only what you need for your business.
3. **Lock it.** Protect the information in your care.
4. **Pitch it.** Properly dispose of what you no longer need.
5. **Plan ahead.** Create a plan to respond to security incidents.

Take Stock

Know what personal information you have in your files and on your computers.

- Inventory all file storage and electronic equipment. Where does your company store sensitive data?
- Talk with your employees and outside service providers to determine who sends personal information to your business, and how it is sent.
- Consider all the ways you collect personal information from customers, and what kind of information you collect.
- Review where you keep the information you collect, and who has access to it.

Scale Down

Keep only what you need for your business.

- Use Social Security numbers only for required and lawful purposes. Don't use SSNs as employee identifiers or customer locators.
- Keep customer credit card information only if you have a business need for it.
- Review the forms you use to gather data — like credit applications and fill-in-the-blank web screens for potential customers — and revise them to eliminate requests for information you don't need.

- Change the default settings on your software that reads customers' credit cards. Don't keep information you don't need.
- Truncate the account information on electronically printed credit and debit card receipts you give your customers. You may include no more than the last five digits of the card number, and you must delete the card's expiration date.
- Develop a written records retention policy, especially if you must keep information for business reasons or to comply with the law.

Lock It

Protect the information that you keep.

- Put documents and other materials containing personally identifiable information in a locked room or file cabinet.
- Remind employees to put files away, log off their computers, and lock their file cabinets and office doors at the end of the day.
- Implement appropriate access controls for your building.
- Encrypt sensitive information if you must send it over public networks.
- Regularly run up-to-date anti-virus and anti-spyware programs on individual computers.
- Require employees to use strong passwords.
- Caution employees against transmitting personal information via e-mail.
- Create security policies for laptops used both within your office, and while traveling.
- Use a firewall to protect your computers and your network.
- Set "access controls" to allow only trusted employees with a legitimate business need to access the network.
- Monitor incoming Internet traffic for signs of security breaches.
- Check references and do background checks before hiring employees who will have access to sensitive data.
- Create procedures to ensure workers who leave your organization no longer have access to sensitive information.
- Educate employees about how to avoid phishing and phone pretexting scams.

Pitch It

Properly dispose of what you no longer need.

- Create and implement information disposal practices.
- Dispose of paper records by shredding, burning, or pulverizing them.
- Defeat dumpster divers by encouraging your staff to separate the stuff that's safe to trash from sensitive data that needs to be discarded with care.
- Make shredders available throughout the workplace, including next to the photocopier.

- Use wipe utility programs when disposing of old computers and portable storage devices.
- Give business travelers and employees who work from home a list of procedures for disposing of sensitive documents, old computers, and portable devices.

Plan Ahead

- Create a plan for responding to security incidents.
- Create a plan to respond to security incidents, and designate a response team led by a senior staff person.
- Draft contingency plans for how your business will respond to different kinds of security incidents. Some threats may come out of left field; others — a lost laptop or a hack attack, to name just two — are unfortunate, but foreseeable.
- Investigate security incidents immediately.
- Create a list of who to notify — inside or outside your organization — in the event of a security breach.
- Immediately disconnect a compromised computer from the Internet.

Protect Your Account

Good practices can keep your information secure.

Corporate Account Takeover is a form of identity theft in which criminals steal your valid online banking credentials. The attacks are usually stealthy and quiet. Malware introduced into your systems may be undetected for weeks or months. Account-draining transfers using stolen credentials may happen at a time when they are not noticed for a day or two.
The good news is, if you follow sound business practices, you can protect your company:

- **Use Layered System Security:** Create layers of firewalls, anti-malware software and encryption. One layer of security might not be enough. Install robust anti-malware programs on every workstation and laptop. Keep them updated.
- **Manage the security of online banking with a single, dedicated computer used exclusively for online banking and cash management.** This computer should not be connected to your business network, should not retrieve any email messages, and should not be used for any online purpose except banking.
- **Educate your employees about cybercrimes.** Make sure your employees understand that just one infected computer can lead to an account takeover. May them very conscious of the risk, and teach them to ask the question: “Does this email or phone call make sense?” before they open attachments or provide information.
- **Block access to unnecessary or high-risk websites.** Prevent access to any website that features adult entertainment, online gaming, social networking and personal email. All such sites can inject files into your network.

- **Establish separate user accounts for every employee accessing financial information, and limit administrative rights.** Many malware programs require administrative rights to the workstation and network in order to steal credentials. If your user permissions for online banking include administrative rights, don't use those credentials for day-to-day processing.
- **Use approval tools in cash management to create dual control on payments.** Requiring two people to issue a payment – one to set up the transaction and a second to approve the transaction – doubles the chances of stopping a criminal from draining your account.
- **Review or reconcile accounts online daily.** The sooner you find suspicious transactions, the sooner the theft can be investigated.

Mobile Security for Business

The most important step in Mobile Banking security is treating your company mobile devices like portable computers. A few common-sense precautions will help protect you from fraud and theft:

- **Set the phone to require a password to power on the handset or awake it from sleep mode.** If it's lost or stolen, any confidential information stored on the device will be more difficult to access.
- **Whether you're using the mobile Web or a mobile client, don't let it automatically log you in to company bank accounts.** Otherwise, if your phone is lost or stolen, someone will have free access to your money.
- **Don't save your password, account number, PIN, answers to secret questions or other such information on the mobile device.**
- **Immediately tell your bank or mobile operator if you lose your phone.** The sooner you report the loss, the better protected you are from fraudulent transactions.
- **Download and install antivirus software for your mobile device, according to the manufacturer's recommendations.**
- **Be careful when downloading Apps.** Downloads should always be from a trusted and approved source, and endorsed by your mobile device provider.
- **Avoid "free offers" and "free ringtones."** An email or instant message that offers free software downloads, such as ringtones, may contain viruses or malware.
- **Be cautious of e-mails or text messages from unknown sources asking you to update, validate or confirm your personal details including password and account information.** Don't reply to text messages from people or places that you do not know.
- **Treat your mobile device as carefully you would your wallet, cash or credit cards.**
- **Keep track of account transactions.** Review your bank statements as regularly as possible to rule out the chances of fraudulent transactions. If you notice discrepancies, contact your bank immediately.

- **Only use Wi-Fi on your device when connected to password protected hotspots.** Turn-off any auto-connect features. They might cause your phone to log into insecure wireless networks without your knowledge.
- **Make sure you log out of social networking sites and online banking when you've finished using them.**
- **Install operating system updates for your device as they become available - they often include security updates.**
- **Before you upgrade or recycle your device, delete all personal/business details.**

Mobile Banking is a very useful tool for your business. By using common sense, it can also be a safe and secure part of your daily operations.

Social Engineering

"Social Engineering" is any method of theft that manipulates human nature in order to gain access to your online financial accounts. No business is immune to the risks of Social Engineering attacks, and thieves will go to great lengths to lower your guard. Here are a few ways you can protect yourself from thieves using Social Engineering techniques:

- **Don't allow unfamiliar visitors into any area with network access.** Thieves often pose as vendors, service providers or even firefighters conducting an inspection, in order to gain physical access to your network. It only takes a few seconds for them to plug in a thumb drive that installs keystroke logging software. Legitimate technicians or officers will have I.D. beyond a logo shirt or uniform to back up their claim, and should be verified independently.
- **Be cautious about letting visitors use a workstation or plug into your network.** A request to "check my email" or "download that sales brochure" might seem innocent enough. But, this is a favorite tactic of Social Engineers to gain access to your network and leave monitoring software or hardware behind.
- **Control access to your facility.** Whatever type of business you are in, there should be barriers between public and private back office areas. Doors leading into back offices from public areas should be locked. Doors to outdoor smoking areas should be locked. Visitors to back office areas should always be accompanied by a trusted employee.
- **Don't assume that an unsolicited phone call or email is actually from a trusted source.** Thieves can research your business relationships or donations, then pose as a vendor or charity you trust. They can even pose as another company employee needing help. Again, verify before providing any confidential information.
- **Remember, unexpected email attachments should be treated with great caution.** Common and popular files like PDFs, JPGs and spreadsheets can provide a platform for installing viruses or keystroke-logging malware on your computer. If you aren't certain the file came from a legitimate business, charity or

person, don't open it without verifying. Call them and ask if they sent an email with an attachment.
- **Verify, verify, verify.** If you receive a phone call or email claiming there is a problem with a bank account, credit card account or any other network or finance related account, hang up the phone or delete the email and check those accounts directly through normal access channels.

The best way to avoid Social Engineering schemes is to be cautious about any unknown visitor, and any request for money, passwords, account numbers or other confidential information – no matter where it seems to be coming from.

Helping you protect the security of information held by your company is as important to us as it is to you. Let's work together to protect it.

Additional Resources

The following links are provided solely as a convenience to our visitors. The bank neither endorses nor guarantees in any way the organizations, services or advice associated with these links. The bank is not responsible for the accuracy of the content found on these sites.

- Identity Theft, Privacy, and Security Publications for Businesses
- National Institute of Standards and Technology (NIST)'s Computer Security Resource Center
- NIST's Risk Management Guide for Information Technology Systems (pdf)
- SANS (SysAdmin, Audit, Network, Security) Institute's Twenty Most Critical Internet Security Vulnerabilities
- U.S. Computer Emergency Readiness Team (US-CERT)
- Carnegie Mellon Software Engineering Institute's CERT Coordination Center
- Center for Internet Security (CIS)
- The Open Web Application Security Project
- Institute for Security Technology Studies