GrandSouth BANK

Best Practices For Businesses Cyber Security Awareness

Introduction

Protect your business with cash management solutions through GrandSouth Bank's Business Online banking platform, Grand Access. The cash management products offered by GrandSouth Bank will make your banking more efficient, secure, easy to use and easily accessible. However, with the increased online access comes the risk of your business's information being compromised through cybercrime.

Cybercrimes are not new; cyber-criminals employ various technological and non-technological methods to manipulate or trick you or other victims into divulging your personal or account information. Such techniques may include performing an action such as getting you to open an e-mail attachment/link, accept a fake friend request on a social networking site, or visit a legitimate, yet compromised, website that installs malware on your computer(s). Modern cybercrime is about money. Cyber criminals are broadening their targets to the financial accounts of owners, employees, small businesses, and medium sized businesses. If these criminals find weaknesses in your cyber practices, significant business disruption and potential monetary losses may result.

You want to be sure you are doing everything you can to protect your business virtually in the same way you protect your business with locks, cameras, and alarm systems. Having protection software is only part of the equation. No single layer of protection is enough; a layered security approach is needed, especially when employees can easily and unknowingly engage in potentially unsafe behavior online. The best practices developed in this handout are intended to raise your awareness of ways to help protect, detect, and educate business employees on today's online risks. We encourage you to understand your unique cybersecurity needs and create a plan suited for your company.

Protect

Secure your Business's Network, Data, and Computers

Dedicate a Computer

Try using one dedicated computer on a safe network to perform your online banking transactions. If a stand-alone device is not possible then ensure that each user of online services uses his/her own device (desktop computer, laptop or mobile) and his/her own password. Sharing computers or logins for accessing financial services is highly discouraged. Sharing a computer that has become infected compromises all users and accounts used on that computer. Best practice for a workstation used for online banking is to eliminate use for general web browsing, emailing and social networking.

Endpoint Protection

Install and maintain real-time anti-virus, anti-spyware, and anti-malware resources. Use these tools regularly to scan your business network and allow automatic updates for your software and operating systems. Be sure your virus detection software, adware and spyware-blocking software are up-to-date.

Firewalls

Install firewall hardware to prevent unauthorized access to your network. Be sure to use Intrusion Detection Systems (IDS) or Intrusion Prevention Systems (IPS) services to detect and prevent attacks from causing harm. It is recommended to have a network/security professional install and maintain firewall systems.

Back-up

It is critical to have a contingency plan to recover files on your

systems that were lost due to a catastrophic system/hardware failure or a cyber-attack (i.e., ransomware) Develop scheduled backups for all critical systems and data, then commit to verifying that the backups are usable by testing their validity on a regular basis. Do not forget to verify that backup data can be restored quickly. If it takes weeks to get backups restored, the business may suffer.

Patch Management

Ensure all computers are updated as soon as possible. (Microsoft releases patches on the second Tuesday of each month) Third party software such as Adobe and Java products are important to update as well.

Secure Data Transfer

When sending sensitive information, email is not to be trusted. Finding a user-friendly email encryption product is important when sending information outside your business.

Wireless

Do not use publicly available internet to access accounts or sensitive business information. (e.g., Internet cafes, public Wi-Fi at airports or government buildings) If this type of access is needed, ensure your transmissions are encrypted. To do this you can employ a Virtual Private Network (VPN).

VPN

Virtual Private Networks can be configured on most firewalls and are very helpful in keeping sensitive data protected. Be sure to protect VPNs with very strong passwords that change often. Contact your network/security professional for proper configuration.

Mobile

Be careful using mobile devices and tablets. While convenient, information technology experts say that in many ways, mobile devices are more vulnerable to unwanted access. Cyber criminals can still steal data that results in identity theft or access to confidential information and banking accounts via phones and tablets despite popular belief.

Categorize and Isolate Information Systems

Keep your business email, payroll system, point-of-sale (POS) system on separate equipment/servers to prevent a compromise from impacting all systems at once. Document and categorize your data assets to manage your network design. Once identified, you can give permission to those who require access to that information.

Insurance

Consult with your insurance agent or carrier about employee dishonesty and cyber insurance coverage. Policy coverage may only be valuable if your corporate security policies are well defined, and procedures are followed. Not all cyber insurance policies are created equal, so it is critical to read and understand the policy details and key definitions to determine what your carrier requires in the event of a security incident.

User IDs, Tokens, Passwords, Controls

Do not share your secure User ID and password with anyone, even with a co-worker. GrandSouth will ask for your User ID when you initiate a call, but GrandSouth will never ask for your password. Never give your password to anyone. Never let anyone watch you log into your bank account, especially while receiving remote support.

Make sure key employees have a trained backup in the event of an absence, who have their own ID and password available to continue banking business as usual. Ensure your bank is aware of the backup's access rights.

- Don't forget to delete employee IDs and access when they leave the business or change responsibilities. Regularly review an active access list and determine any changes to privileges that may be needed.
- Create strong passwords, not something that is easily guessed. Try using a sentence with punctuation, special characters or a mix of letters and numbers. Avoid dictionary words and passwords used in other locations. Try to keep password length over 10 characters when possible.
- Change your passwords often, at minimum based on your company policy. 90 days is a good starting point.
- When you sign into a webpage and are given the option to save your password, select NO.

Dual Control creates safety checks

Initiate ACH and wire transfer payments under dual control using two separate computers. For example: one person authorizes the creation of the payment file, and a second person authorizes the release of the file from a different computer system.

Note: *This helps ensure that one person does not have the access authority to perform both payment functions. Additionally, dual control will ensure that one person cannot give themselves additional authority or create new User IDs.*

Block Sites

Consider enlisting the help of an Internet service to automatically block sites that employees do not need to access for business purposes (i.e., social networking sites, blogs, instant messenger, and free software sites) to reduce the risk of downloading malware or spyware. Most firewalls have this service. Contact your network/security professional for proper configuration.

Check Stock

Maintain controls around physical check stock and ensure that your check supplier has integrated security features embedded in the check stock. Consider alternative forms of payment such as ACH payments, Business Debit or PCard payments to help minimize risk.

Detect

Monitor and reconcile your accounts regularly

Reviewing accounts regularly (daily, if possible) enhances the ability to quickly detect unauthorized activity. The quicker this activity is detected, the sooner you can take action to prevent or minimize losses.

Suspicious Activity

If you detect suspicious activity, immediately cease all online activity and disconnect the device and/or any other network connections (including wireless connections) to isolate the system from the network. From a known trusted device, change all account passwords (e.g., email, bank account, computer).

Immediately call your Account Officer or GrandSouth Cash Management Support to report the suspicious activity.

Note any changes in the performance of your computer(s)

- Significant loss of speed
- Computer “locks up” so the user is unable to perform any functions
- Unexpected rebooting, restarting or the inability to shut down
- Unexpected request for a one-time password, token, or other information in the middle of an online session

Vulnerability Assessments and Penetration Testing

Consider working with security professionals to perform periodic reviews of your network security health so that you can understand and remediate issues to improve your company’s risk profile.

Educate

Ask questions

Cash Management Support is here to help. Use the relationship services phone number at 855.GSB.2233 (855.472.2233) to speak with a trained product specialist from 8:30a.m. to 5:00 p.m. EST.

Be knowledgeable about the online services you use and how they look and work. Call your account representative or cash management support if you are suspicious about any request you receive for login or personal information that is confidential, and if something looks or performs in an unusual way. Test employees by sending out fake phishing emails and offer training for those staff members who need additional support .

Continuously educate employees

Cybercrimes are constantly changing, so software and fraud prevention solutions have to change as well to stay ahead of the game. Determine if you are taking advantage of all the fraud solution options that GrandSouth Bank offers business customers.

Watch our Fraud/ID Theft video

http://www.onlinebanktours.com/mobile/?b=1200&c=21735#Player_Pos

Stay abreast of current fraud risks publicized on one of our fraud partners’ websites. See Cyber Resources on page 4. The online fraud environment changes rapidly so refer to these sites regularly.

Unusual Requests

Wire transfer fraud schemes use social engineering to trick employees into wiring large sums of money to false accounts. Employees should flag strange or unusual requests, even if the request seems to be from a trusted source.

Periodic updates – Hold meetings to review data security. Familiarize new hires with your security protocols to ensure everyone involved learns to spot possible attacks.

Suspicious emails – Don't view or open attachments or click on links in unsolicited e-mails. Financial institutions and government agencies do not contact customers by e-mail or phone asking for passwords, credit card numbers, or other sensitive information. This is also true if you are contacted from an apparent legitimate source (such as the IRS, Better Business Bureau, Federal courts, UPS, etc.).

Be wary of pop-up messages claiming your machine is infected and offering software to scan and fix the problem, as it could actually be malicious software that allows the fraudster to remotely access and control your computer. If the warning is not coming from your own protection service, try to close the pop-up with task manager or when in doubt restart the computer and run a virus scan using your trusted product of choice.

Report suspicious activity – Make sure your employees know how and to whom suspicious activity should be reported both internally and with accounts at your financial institution. Immediately contact your financial institution if you notice unauthorized activity so that the following steps may be taken to:

- Disable online access to accounts
- Change online banking passwords (email and computer password changes are highly recommended)
- Request that the financial institution's agent reviews all recent transactions and electronic authorizations on the account. If suspicious active transactions are identified, cancel them immediately.
- Ensure no new changes have occurred on the accounts such as address changes, added users, or changed PINs.

It is important to note...

- The above best practices will help you protect yourself, your computer, and your organization – but only if all precautions are followed to prevent unauthorized access to your computer and/or login credentials. Once an unauthorized person has gained access, it may be too late to stop their actions.
- Notify your account officer immediately if you discover any unauthorized or unusual activity involving your business or GrandSouth Bank accounts. You may also contact Cash Management Support Services at 855.GSB.2233 (855.472.2233).

CYBER RESOURCES

Stay informed about current threats by having these resource links saved in your browser's favorites.

Internet Crime Compliant Center (IC3) FBI:
www.ic3.gov

United States Computer Emergency Readiness Team:
www.us-cert.gov

Department of Homeland Security:
www.dhs.gov

National Consumers League's Fraud Center:
www.fraud.org

National Check Fraud Center:
www.ckfraud.org

Better Business Bureau:
www.bbb.org/data-security/

The Federal Trade Commission is the nation's consumer protection agency:
www.ftc.gov

Federal Bureau of Investigations:
www.fbi.gov/scams-safety

Homeland Security Cyber Security Research and Development Center:
www.cyber.st.dhs.gov

National Cyber Security Alliance:
www.staysafeonline.org

MEMBER FDIC. EQUAL OPPORTUNITY LENDER.
DISCLAIMER: The suggestions outlined in this document are for informational purposes only. These suggestions are not intended, nor should they be used as an exclusive list of potential solutions aimed at the detection and prevention of cyber-crime and related fraud risks. GrandSouth Bank is not an information technology expert and is not offering specific information technology or other computer systems advice. Accordingly, you and your company should consult your own computer systems or information technology expert(s) to adequately address any and all issues relating to cyber-crime detection and prevention including, without limitation, any potential computer or systems infection, viruses or malware.