BUSINESS

A Few Important Words About

ONLINE BANKING SECURITY

FOR BUSINESSES

As they say, “it’s a jungle out there”. Even for those who keep us up-to-date on system upgrades and follow safe practices. The “bad guys” are working hard every minute across the globe to thwart the latest protections. On top of everything else, you need to stay attentive to what’s happening in your account at all times.

The biggest threat today. A group of bank regulators called the Federal Financial Institutions Examination Council (FFIEC) reports that “malware” is the biggest threat to online financial institutions today. This refers to the many varieties of malicious software that can get inadvertently loaded on your computer and cause trouble – in some cases leading to financial loss. Security researchers found malware targeting online banking on computers at 90 percent of the Fortune 500 companies. Reports indicate that as much as 50 percent of malware goes undetected by anti-virus and anti-malware software. Malware is responsible for millions of dollars in fraudulent financial transactions each month, including incidents right here in Maine. Cybercriminal groups are making headlines with malware programs, such as *ZeuS* and *SpyEye* and their countless variants. For every crime ring that is taken down, countless other groups are actively launching new attacks.

Other security threats. We can’t overlook the “older” methods too, such as “phishing” and “vishing”where criminals contact people via email, phone, social media or text asking for private information and trick them into thinking it is for legitimate reasons. The list goes on…

Gorham
SAVINGS BANK
Banking is believing℠

09.2017

Malware can operate at many levels. "Key logging" is when malware keeps track of your keystrokes and sends whatever you type to criminals tracking you – often as you type! There are malware programs that send out fraudulent financial transactions while you are online, all automatically. Your money may go directly to the fraudster, or in more complex situations it may go to unwitting "mules" who take some of your money and send the rest to the fraudsters, thinking they are working for a legitimate business. Malware can defeat security questions, device ID's, certificates, one-time passcodes and software tokens.

The Bottom Line: be careful, don't be chicken-little. People need to be careful, but don't let this prevent you from utilizing the power, efficiency and convenience of online banking. What's left of paper based financial transactions if quickly fading. So despite the risks, online banking is here to stay.

What It Means To Have A "Layered Approach"

Multiple locks on multiple doors. Multiple layers means having more than just one lock on the "front door". Or taking this a step further, if your online financial transactions were a house, a layered approach means having more than one lock on the front door (such as security questions, tokens, etc) and locks on some of the inside doors too (like the door you open to send a single transaction).

Multiple layers of security at different points in the online banking process make it more difficult for fraudsters to steal money. The FFIEC now requires multiple layers. The number of layers depends on how risky a transaction might be. An ACH or wire transaction is considered riskier than a balance inquiry or even a bill payment. (You can read the FFIEC bulletin on requirements by searching online for "FFIEC Guidance on Internet Banking Authentication".)

Examples of Layers:

- Fraud Detection and Monitoring
- Dual Controls within the business
- "Out-of-Band" Authentication Verification (more on this below)
- Transaction Limits
- Enhanced Control of Administrative Activities
- Employee/Customer Education

A Little More About "Out-of-Band" Authentication

Since Gorham Savings Bank is offers (and requires) an "out-of-band" layer in our security, we thought we'd explain a little more about it. "Out-of-band" simply means that part of the authentication takes place *outside* of bank systems. In our case, we use the phone system. The rationale is that if your information has been compromised by fraudsters, we have at least one step that involves a totally separate system.

For example, when an ACH or wire payment is submitted the first step is an automated phone call to the registered phone number for that account. The user will have to respond to that phone call for the transaction to go through. The phone number assigned to an account cannot be changed without verbal/written authentication by bank personnel. This also satisfies what is called "multi-factor" authentication.

The three factors are:

- Something you know (such as a password or security question),
- Something you have (such as a specific phone), and
- Something you are" (such as a fingerprint or eye scan- we're not there yet).

GSB's "out-of-band" authentication includes two of the three factors.

What Gorham Savings Bank Offers

Let's take the list presented above and briefly describe ways we can help your business reduce risk. Please call us for a more in-depth discussion relating to your own situation.

- **Fraud Detection and Monitoring.** The business has the responsibility to monitor their accounts. Besides what's mentioned below, ultimately only the business will know if a transaction is legitimate. Our online banking system allows businesses to see the details of all transactions with easy download ability into common office software or reconciliation programs. As for automated monitoring, Gorham Savings Bank allows you to set up alerts that notify you each morning when a balance is above or below a certain level. In our ACH and wire systems, you can set up a variety of alerts including alerts for completed, failed or modified transactions. Alerts can tell you if your password or other profile information has changed.

- **Dual Authorization within the business.** Our online banking systems allows the business online account administrator to set up dual controls. This means that one person might have the ability to set up a transaction but not to submit it. Another person might have the ability to submit, but not to create a transaction.

- **"Out-of-Band" Authentication.** The *PhoneVerify* system is required for all business ACH and wire users. This automated system will not allow the user to fully submit an electronic or batch transaction until the customer responds to an "out-of-band" phone call to verify it.

- **Transaction Limits.** Our online banking system allows the business account administrator to set limits for ACH and wire transactions by user. There are daily and aggregate limits. Aggregate limits can be set up to look at different time intervals (weekly, monthly, etc).

- **Enhanced Control of Administrative Activities.** We have other administrative controls including new-user notifications. Let us know and we can talk about these in detail.

- **Employee/Customer Education.** This document is part of our training. We will also provide an overview when we set up a new customer. We are always available to visit your office and discuss risk management, from casual employee discussions to formal Board presentations.

Business Responsibilities & Best Practices

Businesses have important responsibilities.
Mitigating the risks of online banking is not only the responsibility of the bank. Businesses have a variety of responsibilities involving systems, procedures, and equipment. Some businesses feel they should have the same regulatory protections as individuals do, but that is not the case.

Businesses have different protections than consumers.
"Regulation E", the regulation that provides consumer protections from fraudulent transactions, does not apply to businesses. For example, the regulation provides consumers with 60 days to report fraudulent transactions, but businesses do not have this same protection.

Options Every Business Should Consider:

ACCOUNT CONTROLS

- Restrict user access and limits where possible.
- Limit use of admin log in. If the admin will be using the system on a daily basis, consider assigning a separate user name with more restrictive access and limits for daily functions.
- Initiate wire transfers and ACH payments under dual control, with a transaction originator and separate transaction authorizer.
- Review ACH and wire activity logs in online banking at the end of each business day.
- Ensure that all processed batches for the current business day are legitimate.
- Reconcile all transactions on a regular basis. (Daily, if possible.)
- Consider using account services that may aid monitoring account activity, such as Positive Pay and ACH Block/Filter.
- Use the online banking alert system to be notified of transaction activity or changes in your account.

BEST PRACTICES

- Do your own risk audit and control assessment of your business on an annual basis. (Keep your findings – this could be important for outside audits of your company by large customers or audit firms.)
- Consider doing your online banking using a PC with a Linux based operating system, or use a Mac. Both are easy to use and far less likely to be infected with malware.
- If you perform high value or a large number of online banking transactions, consider a stand-along, hardened PC used only for this purpose.
- Be suspicious of emails purported to be from the Bank, a government agency, or any source that is requesting account information, account verification or banking access credentials such as user names, passwords, or similar information.
- Don't open file attachments or click on web links in suspicious emails, as they may expose your system to malicious code.
- If you have broadband or a dedicated connection to the internet, install a dedicated, actively managed firewall.
- Use strong passwords at least 10 characters in length with a combination of letters, numbers, and special characters.
- Prohibit the use of "shared" usernames and passwords for online banking access.
- Change your password regularly.
- Limit administrative rights on users' workstations to help prevent the inadvertent downloading of malware and other viruses.
- Ensure virus protection and other security software is updated regularly, as well as operating system and key application security patches. Consider installing spyware protection programs.
- Verify use of a secure session (*http***s** not *http*) in your browser for all online banking.

- Avoid using automatic login features that save usernames and passwords for online banking.
- Familiarize yourself with your account agreement and Cash Management Master Services Agreement. A good understanding of these will aid in answering any questions you have regarding roles and responsibilities related to the use of online banking.

NOTIFICATION

- Notify and train staff with access to online banking so they can take precautionary steps.
- Notify the Bank if you receive any communication requesting account information or access credentials.
- Immediately escalate any suspicious activity or transactions to the attention of the Bank, particularly wire transfers or ACH.

Who To Contact In The Event of Suspicious Activity

If you have any questions, or want to report suspicious activities,
please use the information below to contact us:

Customer Service Center
(207) 839-4796 or (800) 492-8120
CustomerService@GorhamSavingsBank.com
Monday - Friday 7:30AM- 5:00PM
Saturday 7:30AM - 12:00PM

For all other hours, please call:
ATM/Debit Cards (800) 500-1044
Credit Cards (800) 883-0131