Jonah Bank of Wyoming Security offerings guide

This guide was created to increase our customer's awareness of the potential risks and threats that are associated with internet and electronic-based services, and to provide solutions and tools to help prevent fraud and scams

Overview

1. Types of Fraud
2. Jonah Bank Security Controls
3. Customer Security Controls
4. Customer Acknowledgement

1. Types of Fraud

With the types, sophistication and breadth of cybercrime increasing and evolving each year, it is important that you be aware of the trends in Cybercrime that can impact your business. When focusing on fraud that can affect your bank accounts it is important to remember that it is a joint effort between you and your bank to help Protect, Detect and Respond to fraud.

CATO

Corporate **A**ccount **T**ake **O**ver is a fast growing electronic crime where thieves typically use some form of malware, or malicious software, to obtain login credentials to corporate online banking accounts and fraudulently transfer funds from the accounts or steal other sensitive information. Another means fraudsters commonly employee is phishing, masquerading as a trustworthy entity in an electronic communication or through social engineering to gain access to your sensitive information.

These attacks can result in substantial monetary loss for your company that, often, cannot be recovered. As a bank, we do everything we can to keep your money safe. Unfortunately, our security practices can only go so far to protect your accounts from corporate account takeover. There are some vulnerabilities that can only be addressed from the company side and therefore require that the business implement sound practices with their staff, systems and offices. These practices are discussed below with each tool attackers use, and at the end under Customer Security Controls.

Due to the high risk of CATO, Jonah Bank has developed an entire guide that is available to you:

https://www.jonah.bank/sites/www.jonah.bank/files/jonahbankcatoguide.pdf

Check Fraud

Check fraud has been around for as long as there have been checks, its simplicity and low tech nature are what keep it as one of the most prevalent forms of fraud affecting business accounts. The 2014 AFP (Association for Financial Professionals) Payments Fraud and Control Survey found of all businesses who experienced fraud or attempted fraud checks were the primary target (81%).

Check fraud includes the altering of checks, forged endorsements, counterfeiting, unauthorized use of, or re-issuance of checks, check kiting and third party bill payment services. The number one control a business can take to protect against check fraud is to implement Positive Pay (81% of business in the AFP study cited this as their primary control). Other steps businesses should take include:

- Maintaining sufficient controls for check storage, issuance and reconciliation
- Notify Jonah Bank in a timely manner when fraud occurs
- Review bank statements
- Reconcile accounts
- Use standard fraud protections (such as Positive Pay)
- Reduce the number of checks written by taking advantage of ACH and Bill Pay capabilities

Loan and Social Security Fraud

Loan and Social Security fraud are types of fraud where criminals have gained access to your personal information and are using it to take out loans, and credit cards in your name to later use fraudulently. This type of fraud is commonly known as Identity theft. While there are many sites that store your personal information, it is important to remember that for business accounts, Cyber Criminals have the ability to obtain access to the personal information of all of your employees, and thus they are at a higher risk.

To prevent against identity theft companies should implement all available forms of protection offered by entities where Personal Information is stored. When it comes to protecting Personal Information stored within Jonah Banks Online Banking System you should implement the following security measures:

- Strong Passwords
- Out-of-Band Authentication at login – such as requiring Secure Access Codes, and not registering your browser
- Creation and monitoring of security alert preferences that can tip you off to someone logging into your account, changing a password or logging in from a different device among others. (For assistance with setting these up please contact a customer service representative).
- Use of dedicated computers for online banking.
- Limit the number of authorized users
- Limit the capability of authorized users
- Ensure that basic PC security measures are taken, such as updating the operating system, browser, and third party applications in a reasonable time frame, and ensure that Antivirus, Anti-Malware and personal firewalls are all installed and up to date.

2. Cyber Criminal Tools

Cyber criminals have a vast array of tools for gathering information and perpetrating fraud. As technology evolves these tools are becoming more prevalent, sophisticated and targeted, while at the same time becoming increasingly accessible for even novice cybercriminals to purchase and use. The Symantec 2014 Internet Security Threat report reveals how important it is becoming for businesses of all size to take action against cyber threats. The key findings of the ISTR 2014 report were:

- 91% increase in targeted attack campaigns in 2013
- 62% increase in the number of breaches in 2013
- 8 breaches with more than 10 million identities were exposed
- Over 522 Million Identities exposed via breaches in 2013
- 38% of mobile users have experienced mobile cybercrime in past 12 months
- Spam volume dropped to 66% of all email traffic
- 1 in 392 emails contain a phishing attack
- Web based attacks up 23%
- Ransom ware attacks up 500%
- These attacks whilst not all on financial institutions and their customers resulted in:
    - $9,761 in fraud committed against US FIs every 60 seconds
    - $4.9B Online account fraud reported by US FIs in 2013 (2013 Faces of Fraud Survey)

To develop a strategy for defending against cyber criminals we need to know their methods of attack and the ways we can protect against them.

Social Engineering

Social Engineering is the use of deception and manipulation to obtain confidential information. It is a non-technical kind of intrusion that relies heavily on human interaction and often involves tricking people into breaking normal security procedures. Social engineers rely on the fact that people are not aware of the value of the information they possess and are careless about protecting it. The attacker's goal is to obtain information that will gain him/her unauthorized access to a system and the information that resides on that system. Typical examples of social engineering are phishing e-mails, pharming sites, poisoned search results, fraudulent donation requests, and malware on social networking sites.

To defend against social engineering attacks and protect your company and online banking credentials companies should:

- Educate their staff about social engineering, and the importance of not providing information, even trivial, to non-authorized individuals, this could include how to handle telephone calls, social media services and mail.
- Verify the identity of vendors performing any work on premise
- Apply the "If it is too good to be true, it probably is" mentality to all offers
- Use the Stop-Think-Click approach for all email links and attachments
- Implement a content filter – this can greatly reduce the probability of following malicious search results.
- Shredding of business documents that are no longer needed, and use eStatements
- Never sharing passwords, and to make them strong and unique.

Phishing

Phishing is the method used to steal personal information through spamming or other deceptive means. There are a number of different phishing techniques used to obtain personal information from users including email/spam, Man-in-The-Middle, Key Loggers, Search Engine phishing and malware phishing. Typical phishing techniques use an urgent call to action to provoke the recipient into divulging information or clicking on a link or attachment that they typically would not.

The number of phishing emails actually decreased in 2013, however the number of targeted phishing campaigns (Spear-Phishing) increased by 91%. This increase in targeted phishing campaigns is in part related to the increasing sophistication of their tools and use of already stolen information. By targeting smaller groups users in a targeted attack, cyber-criminals have been able to stay under the radar of some spam filters, and have had higher success rates with using messages that are tailored to a particular users industry or job role.

To protect against phishing attacks companies and their users can:

- Scrutinize email carefully – verify links, and attachments, look for grammar and spelling mistakes, and question the context of the email
- Never enter financial or personal information in websites provided as links in email messages
- Use Anti-Spyware software, firewalls and content filters
- Never send personal information via email
- Never download files from unreliable sources
- Check bank details regularly
- Be wary of pop-ups

Vishing

Unfortunately, phishing emails are not the only way people can try to fool you into providing personal information in an effort to steal your identity or commit fraud. Criminals also use the phone to solicit your personal information. This telephone version of phishing is sometimes called Vishing. Vishing relies on “social engineering” techniques to trick you into providing information that others can use to access and use your important accounts. People can also use this information to pretend to be you and open new lines of credit.

To protect against Vishing, we recommend that you apply the same prevention techniques as for Social engineering and Phishing, with additional control, and that is If you receive an email or phone call asking you to call a number back, and you suspect it might be a fraudulent request, look up the organization’s customer service number and call that number rather than the number provided in the solicitation email or phone call.

Smishing

Just like phishing, Smishing uses cell phone text messages to lure consumers in. Often the text will contain an URL or phone number. The phone number often has an automated voice response system. And again just like phishing, the Smishing message usually asks for your immediate attention.

In many cases, the Smishing message will come from a "5000" number instead of displaying an actual phone number. This usually indicates the SMS message was sent via email to the cell phone, and not sent from another cell phone.

Malware

Often delivered by malicious email links or drive by downloads on insecure websites, is short for "malicious software." Malware is any kind of unwanted software that is installed without your adequate

consent. Viruses, worms, and Trojan horses are examples of malicious software that are often grouped together and referred to as malware.

In 2013 Symantec's IST Report showed that Ransomeware attacks grew by 500%, and financial malware tripled in the first quarter of 2013 alone. Just like phishing, Malware can be installed by presenting an urgent message to the user requiring their immediate action. This is commonly seen in fake Antivirus windows and the CryptoLocker virus. Malware can also be installed by visiting poorly secured websites, or via malicious links in search results and Malvertisements.

To defend against Malware we recommend you take the following actions:

- Ensure all systems and network devices are regularly updated
- Implement a patch management strategy for all third party applications, such as Java, Adobe Reader, Adobe Flash etc. (unpatched systems are the largest attack vector for malware)
- Install and maintain Antivirus, AntiMalware and Firewalls
- Don't open Spam email messages or click on links on suspicious websites
- Implement a well thought out backup strategy
- Enforce the use of strong passwords.

Mobile

In 2013 Symantec reported that 38% of mobile users were the victim of mobile cybercrime, and the increase in MadWare (Mobile Adware) grew at an increased rate as mobile adoption continued it's rapid pace. With the adoption rates of mobile devices continuing to skyrocket, and the increased amount of information being stored on or accessible from mobile devices it is little wonder why Cyber-Criminals have increasingly targeted mobile devices. When it comes to mobile threats and security, the same threats exist as for these devices as exist on traditional computers.

To defend against mobile threats:

- Implement the same general computer security precautions you currently use on your traditional computer – update the operating system and applications, be suspicious of text's, pushed messages and emails.
- Perform vendor review of Apps before downloading them – in April of 2004 Google took down the #1 app in its google play store as it was deemed to be a malicious app masquerading as a security/antimalware utility "Virus Shield"
- Develop a thorough mobile device usage policy that details the acceptable use of mobile devices, what information can and cannot be stored on them, the use of security features such as PIN locks, and Find my phone capabilities.

3. Jonah Bank Security Controls

We take protecting your accounts and personal information on Jonah Bank's Online Banking system very seriously, and we have taken every effort to provide you with a safe and secure experience. In developing the security tools available within Online Banking, Jonah Bank takes a Defense in depth approach to securing and safeguarding your information, because no single control by itself is effective. Below you will find various tools you can use to protect your accounts, and some information of

enforced minimum requirements that we maintain. As you read through each of the items, keep in mind that it is Jonah Bank's recommendation that each of the tools be used in its entirety and in conjunction with safe computing habits.

Passwords

The use of strong passwords is an essential first step in protecting your accounts. We recommend creating a password of at least eight characters that is comprised of Upper Case, Lower Case, Numerals and Symbols, and does not include common dictionary words, sequential or repeating characters. We also recommend that these passwords be changed at a minimum of every 90 days, that they be unique to any other password used for any other system that you interact with, that they not be shared or written down in an easily accessible location (either physically or virtually).

When it comes to passwords, please remember that Jonah Bank of Wyoming or any of its staff will NEVER ASK YOU FOR YOUR PASSWORD OR TRANSACTION AUTHORIZATION CODES, and such requests should be treated as highly suspicious, and be a cause for you to IMMEDIATELY CONTACT JONAH BANK using our main line and ask for a customer support specialist. *For more information on creating strong passwords please review the Fighting-Fraud page at https://www.jonah.bank/fighting-fraud.*

Secure Access Codes (SAC's)

When logging into Jonah Bank of Wyoming's Online Banking system for the first time from a new computer, browser or mobile device users are required to receive and enter a Secure Access Code. This process is also known as Out-of-Band Authentication at Login. While it is convenient to elect to register a browser or device after successfully entering a SAC, current financial malware has been shown to steal the cookies from computers, which can later be used by cybercriminals. As a best practice Jonah Bank recommends that you always elect to not register your browser. *For assistance with enforcing SAC's at every login please contact Jonah Bank.*

Transaction Authorization Codes (TAC's)

When authorizing an ACH or Wire transaction, Jonah Bank requires customers to receive an out of band Transaction Authorization Code via voice or SMS (text message). This ensures that only users with registered code delivery details can authorize transactions on the businesses behalf. Jonah Bank recommends that these codes be used for ALL ACH and Wire transactions regardless of the dollar amount. *For assistance with setting up TAC's please contact Jonah Bank.*

Dual Approval

Dual Approval is a process where the transactions entered and authorized by one user have to be approved by a second user. When setting up dual approval, you have the ability to enforce dual approval for all transactions, or only those exceeding a specific dollar amount. You can even specify that some users can only approve and not draft transactions. Dual Approval is a great fraud fighting tool, as it protects you in the event that one users credentials have been compromised but a second approving individuals account remains unaffected. *For more information on, and help with setting up Dual Approval please contact a Jonah Bank customer service representative*

Call Backs

To protect high risk wire transfer transactions, Jonah Bank has instituted a compulsory call back process for all wire transactions whether domestic or international.

User Rights

Within your company you may have multiple employees with access to your online bank accounts. If each of these users requires a different set of features (ability to view certain accounts, make funds transfers, ACH payments or Collections, Wires, Bill Pay, Statement access etc.) it is possible to configure each users access to provide access only to the functions required by their job role with your business. By limiting what each user can do in the system, you limit the amount of damage that could be done if a user's credentials were compromised. *For more information on configuring user rights please contact Jonah Bank.*

User Limits

As with User Rights, User Limits allow you to specify maximum dollar amounts for transactions that your staff can draft and authorize (Ideally this limit would be below the maximum amount authorized for your business with Jonah Bank). For larger dollar amounts users may need to have another staff member with higher limits complete the transaction or have the business owner complete the transaction. By limiting the dollar amount of transactions, you decrease the impact of a fraudulent transaction if a user's credentials are compromised. *For more information on configuring user limits please contact Jonah Bank.*

Transaction Alerts

Transaction alerts are a great method to keep you informed of activity within your account as it happens. You can configure alerts for certain accounts, transactions types or dollar amounts. These are a great method to detecting possible fraudulent activity. *For more help with configuring transactions alerts please contact Jonah Bank.*

Security Alerts

Security Alerts inform you when certain security related events occur, such as failed login attempts, when someone attempts to use the forgot password option, or when someone attempts to navigate Browser registration. In a nutshell it alerts you to someone trying to gain access to or modify your online banking account. *For more help with configuring security alerts please contact Jonah Bank.*

Positive Pay

When it comes to protecting your business from check fraud the best defense you can have is to setup Positive Pay. With Positive Pay you can upload a check run file into our Positive Pay system and then be alerted to any exception items as they occur, giving you time to review and action possible check fraud. Exceptions can be generated based on differences in Payee, Date, Amount or Check number. If you are not looking at all of your accounts everyday there is a possibility that check fraud can slip through the cracks, and with only a 24 hour window to dispute a fraudulent check (UCC 4a) time is of the essence. With positive pay you won't miss a fraudulent check. Additionally our Positive Pay system allows you to monitor ACH transactions for possible fraud as well as provide you with reverse positive pay capabilities.

Bill Pay and e-Statements

While not strictly security features of our online banking system, Bill Pay and e-Statements can help protect your business. By using Bill Pay instead of writing checks, you decrease the number of your checks in circulation that could be susceptible to alteration, duplication or forgery. E-Statements are a method to stop mail theft fraud, dumpster diving, and inadvertent disclosure by leaving sensitive information in easily accessible areas.

Behavioral Analytics

Great security, is security that is non-invasive. At Jonah Bank we have a behavioral based analytical engine that is capable of scoring all your activity within our online banking system. This engine looks for anything that is out of the ordinary such as higher than average transaction amounts or volume, or suspicious behavior such as new payee's or changed payee details. When it detects out of the ordinary behavior it flags that transaction as suspect, and requires a Jonah Bank employee to verify its authenticity via a voice phone call.

SSL Protected Online Banking Site

The Jonah Bank website is protected by a 256bit encrypted SSL site certificate. Once on our site you should see the URL begin with "https" and depending on your browsers the URL field should turn green and the locked padlock symbol appear. This means that all communication between you and our site is encrypted.

Customer Security Controls

Implementing all of the security features available to you via Jonah Bank's Online Banking System is a good first step. It is important to remember that it is a joint effort between you and Jonah Bank to help Protect Detect and Respond to fraud. With this in mind we have developed a shortlist of security measures you should implement. Keep in mind that you should aim to implement as many of these control measures as possible to provide the highest level of protection (keep in mind no system is foolproof). *For more detailed information on security please visit our Fighting-Fraud page at https://www.jonah.bank/fighting-fraud.*

Passwords

Enforce strong passwords that are at least 8-10 characters long and include a mixture of letters and numbers. Encourage users to avoid re-using the same passwords on multiple websites and sharing of passwords with others should be forbidden. Passwords should be changed regularly, at least every 90 days. The use of Out of Band Authentication (also called dual factor authentication) should be used whenever available. To assist users with keeping their passwords secure and to make their life a little easier consider the use of Password Wallets

Network Security and Firewalls

When it comes to securing your business computers it all starts at the network. The network is the entry point and exit point for all the data you are sending and receiving, as such you should take some basic measures to ensure that your network is safe. These measures can include:

- Routers - Change the default password on your router, most commercial and consumer routers come with default passwords attached to the Admin account, and these can easily be found online, as such you should change them.
- Wireless - use strong security settings, at a minimum WPA2, more advanced functions would include limiting the number of wireless devices that can connect to your network, the time of day devices can connect, and restricting the devices that can connect to known devices using MAC addresses
- Intrusion Detection and Firewall - Commercial customers should consider implementing both a Firewall at the network level and an Intrusion Detection System, and of course monitor their logs. Firewall software should also be implemented at the client computer level.
- Testing - Commercial customers should consider testing their network for vulnerabilities by conducting Penetration tests and Internal Vulnerability scans. These tests can be a valuable tool in determining where your weaknesses lie.
- For more information on how you can protect your network consult your Internet Service Provider

Operating System and Software Patches

As vulnerabilities are identified by both software vendors and cyber-criminals, updates and patches are made available by software vendors to patch their software to close a vulnerability. As such all companies should develop a sound patch management policy that details the patching of operating systems, network devices, and third party applications. With unpatched systems being the main target of Malware, this step cannot be understated.

Anti-Malware and Anti-Virus Software

Although the installation and updating of Anti-Virus and Anti-Malware software will not protect you from every threat, it is a must have layer in the defense of your network and devices. Ideally your Anti-Virus and Anti-Malware software will be configured to automatically update. When deploying Anti-Malware and Anti-Virus software don't forget about mobile endpoints or shared resources.

Mobile Devices

Ensure that all devices that connect to your corporate network, or have access to corporate data have adequate security precautions in place. These can range from encryption, to Anti-Virus, remote Wipe/Lock functionality and PIN based protection.

Backups

To protect against threats such as Crypto Locker and other scareware, develop and implement a sound backup strategy to protect your data.

Removable Media and Encryption

Implement a removable media policy detailing the allowed use of removable storage. Ideally this policy would require removable media be encrypted to prevent accidental leakage of information in the even a device is lost or stolen. Further think about using encryption on all data whether at rest or in motion.

User Education

Probably the most effective measure you can take in fighting cybercrime is to ensure you have a well-educated and security conscious staff. Education should focus on everything from company acceptable use policies, to secure use of social media, online banking systems, password requirements, email best practices to avoid phishing and social engineering scams, and safe browsing habits.

Testing

Even after implementing sound security practices organizations should routinely test their security through Penetration tests, Vulnerability assessments, Risk Assessments, and Social Engineering exercises.

4. Jonah Bank Customer Acknowledgement

By signing below you are acknowledging that you understand the various threats that surround online banking, the protections that Jonah Bank offers and security controls that you can put in place as described in sections 1 through 3 of this document.

Signature: _____ Date:_____

Your Name: _____

Title: _____

Company: _____

5. Additional Resources

For your reference we have provided the following resources for additional information regarding fraud and security:

- Jonah Bank's *Fighting-Fraud* page. Accessible on our website at *https://www.jonah.bank/fighting-fraud.*
- Jonah Bank's CATO Guide 2014. Accessible at https://www.jonah.bank/sites/www.jonah.bank/files/jonahbankcatoguide.pdf
- Federal Trade Commission(FTC) Federal Governement ID Theft Response Guide. http://www.consumer.ftc.gov/features/feature-0014-identity-theft
- FTC Business Guide for Protecting Data. https://www.ftc.gov/tips-advice/business-center
- Fraud Advisory for Business Corporate Account Take Over http://www.ic3.gov/media/2010/CorporateAccountTakeOver.pdf
- OnGuard Online http://www.onguardonline.gov/
- US-CERT Tips for avoiding Social Engineering and Phishing Attacks http://www.us-cert.gov/ncas/tips/ST04-014