Security Matters

Brought to you by
the Treasury Management
team at Citizens & Northern Bank

Creating value through lifelong relationships

CITIZENS & NORTHERN BANK
Your Bank for a Lifetime

Welcome.

Welcome to our Security Matters newsletter for businesses. Here you will find valuable information about how to limit your company's risk for fraud. We offer a wide variety of products to help keep your account information safe and secure. There's also a great deal you can do to help us help you.

If you do feel your business has been a victim of fraud, contact us immediately. We also welcome your calls with any questions or concerns you may have.

Connect with us.

Feel free to contact a member of our Treasury Management team directly:

Chrissi Hume
90-92 Main Street,
Wellsboro, PA
(570) - 723 - 2173
chrissih@cnbankpa.com

Denise Manley
90-92 Main Street,
Wellsboro, PA
(570) - 723 - 2175
deniseam@cnbankpa.com

Renée Tevlin
90-92 Main Street,
Wellsboro, PA
(570) - 723 - 0239
reneet@cnbankpa.com

ACH Debit Block

Important:

Businesses are not protected under Reg E and only have 24 hours to identify an unauthorized withdrawal and notify the bank. Once that 24 hour period has passed they must recover funds directly from the company or person that charged them.

Did you know...

...In 2018, 78% of companies were targets of payment fraud, 28% were subject to ACH debit fraud and 13% were subject to ACH credit fraud.*

Businesses typically only have 24 hours to return an ACH that is unauthorized. After 24 hours the item can't be returned and the business has to resolve the issue with the ACH originator. That's why we offer products like ACH Debit Block.

With ACH Debit Block we can notify you each time an ACH is drawn on your account or we can customize the notification to fit your needs. Let ACH Debit Block do the monitoring for you!

Any size company or business can benefit from this service in order to safeguard funds from fraudulent electronic transactions.

We offer the following options:

- Block all ACH debit transactions for each specified account.
- Block ACH debit transactions by type; for example WEB (web initiated transactions) or TEL (Telephone initiated transactions).
- Block all ACH debits that do not match your approved vendor list.

*2018 AFP Payments Fraud and Control Survey Report

www.cnbankpa.com 1-888-322-2193 contactcn@cnbankpa.com

Positive Pay

Positive Pay can drastically reduce your risk of financial loss due to check fraud. This automated fraud detection tool reviews every check presented against the account and compares it to a previously authorized and issued list from your company. When verifying validity of the presented checks, the account number, check number and dollar amount must match exactly or the check will not be paid.

Here's how it works:

- Upload your Check Issue File to Citizens & Northern via Online Banking.
- The Daily Incoming Check File will be compared to your Check Issue File.
- We will match the check number and issued amount.
- Exception items (unmatched items) are reported to you each morning.
- You make the decision whether to return or pay the unmatched items.

Did you know...

...Checks remain the payment type most vulnerable to fraud attacks.

...74% of organizations affected by payments fraud report that checks were targeted.

..54% of BEC scams targeted wires, followed by checks at 34%.

**2018 AFP Payments Fraud and Control Survey Report*
***Business Email Compromise (BEC)*

www.cnbankpa.com 1-888-322-2193 contactcn@cnbankpa.com

Online Security

Important:

Business accounts are the most vulnerable to hacker attacks and the least protected by the law. Hackers are much more inclined to break into a six-figure business account than a consumer account with a few thousand dollars.

Security Alerts

In an effort to safeguard your financial information, many security alerts are available via our Online Banking System. These alerts can be set up to contact employees when Payroll, ACH payments or other transactions are initiated.

We offer both Transaction and Security alerts. Within online banking, transaction alerts are located under "Preferences," then "Alerts." You can choose all or several of the seven available alerts. Once you have made your selections, an email, phone call or text message will be sent to the Online Banking user at a designated time.

Security alerts are located under "Preferences," then "Security." You can choose all or several of the 15 available alerts.

Any size company or business can benefit from this service in order to safeguard funds from fraudulent electronic transactions.

Once your alerts have been set up, an email, phone call and/or text message will be sent to the Online Banking user at the time the specified security event takes place.

Security Tokens

Security tokens are online credentials that add an extra layer of identity protection for the authorization of ACH and wire transfer transactions. These portable devices are lightweight and easy to manage. For Smart phone users, a free application can be downloaded and used in place of the physical token device. We recommend the use of security tokens.

Dual Control

Our Online Banking system has the ability to require dual controls for Automated Clearing House (ACH) and wire transfer transactions. Dual control reduces the risk of fraud, promotes funds security and is easy to implement. The feature requires that two different employees be involved in the process. This feature is optional, but we strongly recommend it.

IMPORTANT: Dual Control Reduces the risk of fraud and promotes security by requiring that two different users, each with their own User ID and Password, touch high risk transactions.

Important:

Just as you would never ask a stranger to mail your bills, you should never log into a public computer or use unsecured Wi-Fi to pay bills online.

Business Bill Pay

Paying bills online offers more benefits than saving the cost of a stamp or eliminating the paper trail. It also allows for constant and convenient monitoring. Account transactions show up online right away, allowing you to detect and quickly react to suspicious activity. Tracking and e-mail notifications advise when a bill payment is received and credited, so you don't have to worry about your checks being late or lost in the mail.

In addition to the security advantages, our Online Bill Pay lets you control what is paid, how much is paid and when it's paid.

Advantages of C&N's Online Business Bill Pay

- Make payments more quickly and easily and gain greater control over cash flow
- Get anytime, anywhere access online for more convenience paying your bills
- Save time by conveniently importing payees from Quicken® or Quick Books®
- Pay multiple invoices for a single payee all at one time and account for them in a single location
- Easily set up recurring payments for monthly bills
- Run audit reports and customize them for the precise payment information you need
- Track your company spending and payment history in just a few clicks
- View the payment activity of authorized users and keep track of the payments they have made
- Greatly reduce your paperwork and minimize manual record keeping

www.cnbankpa.com 1-888-322-2193 contactcn@cnbankpa.com

Important:

Citizens & Northern uses a combination of safeguards and sophisticated programs to detect, track, and block unauthorized access to your financial information. While we provide strong data protections, our customers are the first line of defense. This is why a partnership between us and our customers is the most effective way to protect financial data.

Securing Your Personal Information

- **Create c0mplic@t3d passwords.** Create a passphrase instead of a password for securing your information. We recommend using a passphrase instead of a password, because passphrases provide the best combination of memorability and security. They are easier to remember than random symbols and letters. A passphrase is made up of a series of random words or a sentence. Here's an example: "time for tea at 1:23" or "Aren't tigers awesome". Remember, don't share your passphrase with family members and be mindful of who has access to your personal information.
- **Continually monitor accounts.** Check account activity and online statements often, instead of waiting for the monthly statement. You are the first line of defense because you know right away if a transaction is fraudulent. If you notice unusual or unauthorized activity, notify us right away.
- **Protect yourself online.** Be sure computers and mobile devices are equipped with up-to-date anti-virus and malware protection. Never give out your personal financial information in response to an unsolicited email, no matter how official it may seem. We will never contact you by email asking for your password, PIN, or account information. Only open links and attachments from trusted sources. When submitting financial information on a website, look for the padlock or key icon at the top or bottom of your browser, and make sure the Internet address begins with "https."

Reporting Fraud

If you're a victim of fraud & suspect your personal information has been compromised, you should take the following steps:

1. Call your bank and credit card issuers immediately so they can take necessary steps to protect your account.
2. File a police report and call the fraud unit of the three credit-reporting companies.
3. Consider placing a victim statement in your credit report.
4. Make sure to maintain a log of all the contacts you make with authorities regarding the matter.
5. For more advice, contact the FTC's ID Theft Consumer Response Center at 1-877-ID THEFT (1-877-438-4338) or www.ftc.gov/idtheft.
6. IMPORTANT: It is critical that you understand the online threats to your company's network. Awareness of key threats will enable you to employ practices and behaviors that limit your company's risk.

Risk Assessment & Controls Evaluation

Important:

Protecting the confidentiality, integrity, and security of financial services transactions is shared by the bank and your business. A Risk Assessment outlines recommended security controls essential to minimizing the risk of these transactions.

For your convenience we have created an easy-to-use form to ensure that optimal security is in place in your business on the next page.

Business Email Compromise (BEC)

Business Email Compromise is a form of email fraud that typically involves targeting employees with access to company finances and tricking them into making money transfers to the bank accounts of the fraudster. Last year's Internet Crime Report ranks this type of attack as #1 and it represents 48% of total loses in Internet Crimes.

How do you avoid these types of attacks?

1. Look out for domain name spoofing, emails that appear to be from a trusted email address.
2. Look out for display name spoofing, emails that appear to be from somebody you trust.
3. Look out for domain name spoofing that looks like legitimate domains.
4. Never open emails, click on links, or download files from unknown senders.
5. Be careful what you share on Social Media, don't use your business email address on your social media accounts.

As a business owner, you want to make sure you have a very strong process in place for monitoring and managing who has access to your business e-banking services and how that information is handled.

Business customers are encouraged to perform risk assessments periodically (annually at a minimum).

The risk assessments should include a review of the following items at a minimum:

- Bank Account Access and Rights
- User Access Rights
- Token Usage
- ACH and/or Wire Transfer Daily Limit Amounts
- Dual Control Usage

Business E-Banking Risk Assessment and Controls Evaluation

For each question, select the answer(s) that best represent(s) your environment. Following the assessment, use the "Control Evaluation - Best Answers and Tips" to evaluate your environment. Once you have completed the questionnaire, add up the totals following the answers selected to see a summary risk rating of your environment. Note: This rating is designed to give a general idea of your risk posture based only on the answers in this questionnaire. Additional factors could either increase or decrease your risk.

PERSONNEL SECURITY

1) Are employees required to sign an Acceptable Use Policy (AUP)?
   a) Yes, at least annually or more frequently as needed (1)
   b) Yes, but only upon hire (2)
   c) No (5)

2. Does each employee using Online Banking go through security awareness training?
   a) Yes, at least annually or more frequently as needed (1)
   b) Yes, but only upon hire (2)
   c) No (5)

3. Do you run background checks on employees prior to hire?
   a) Yes, for all employees (1)
   b) Yes, but only based on position (2)
   c) No (5)

COMPUTER SYSTEM SECURITY

4. Do computer systems have up-to-date software?
   a) Yes, all systems (1)
   b) Yes, but only critical systems (3)
   c) No (5)

5. Is there a process in place to ensure software updates and patches are applied (Microsoft, web browser, Adobe products, etc.)?
   a) Yes, a formal process where updates are applied at least monthly (1)
   b) Yes, but informally as needed (3)
   c) No (5)

6. Do users run as local administrators on their computer systems?
   a) No (1)
   b) Only those that require it (3)
   c) Yes (5)

7. Is there a firewall in place to protect the network?
   a) Yes (1)
   b) No (15)

COMPUTER SYSTEM SECURITY (Continued)

8. Do you have an Intrusion Detection/Prevention System (IDS/IPS) in place to monitor and protect the network?
   a) Yes (1)
   b) No (3)

9. Is Internet content filtering being used?
   a) Yes, Internet traffic on the system used for "high risk" Online banking activities is completely restricted to only sites specifically needed for business functions (1)
   b) Yes, we have Internet content filtering (2)
   c) No (5)

10. Is e-mail SPAM filtering being used?
   a) Yes (1)
   b) No (5)

11. Are users of the Online banking system trained to manually lock their workstations when they leave them?
   a) Yes, and the systems are set to auto-lock after a period of inactivity (1)
   b) Yes, but it is only manually (2)
   c) No (5)

12. Is wireless technology used on the network with the online banking system?
   a) No (1)
   b) Yes, but wireless traffic uses industry-approved encryption (i.e. WPA, etc.) (1)
   c) Yes, but wireless uses WEP encryption (2)
   d) Yes, and wireless traffic is not encrypted (15)

PHYSICAL SECURITY

13. Are critical systems (including systems used to access online banking) located in a secure area?
   a) Yes, behind a locked door (1)
   b) Yes, in a restricted area (2)
   c) No, in a public area (5)

14. How are passwords protected?
   a) Passwords are securely stored (1)
   b) Passwords are written on paper or sticky notes and placed by the computer (15)

Overall Risk Rating

Low Risk: 0-15
Medium Risk: 16-25
High Risk: 26-35
Extreme Risk: 35+

Business E-Banking Risk Assessment and Controls Evaluation

Following are the results from the risk assessment. Review your answers and the tips to help you protect your systems and information.

1. The best answer is a) Yes, at least annually or more frequently as needed. An Acceptable Use Policy (AUP) details the permitted user activities and consequences of noncompliance. Examples of elements included in an AUP are: Purpose and scope of network activity; devices that can be used to access the network, bans on attempting to break into accounts, crack passwords, circumvent controls or disrupt services; expected user behavior; and consequences of noncompliance.
2. The best answer is a) Yes, at least annually or more frequently as needed. Security Awareness Training (SAT) for online banking users, at minimum, should include a review of the acceptable use policy, desktop security, log-on requirements, password administration guidelines, social engineering tactics, etc.
3. The best answer is a) Yes, for all employees. Companies should have a process to verify job application information on all new employees. The sensitivity of a particular position or job function may warrant additional background and credit checks. After employment, companies should remain alert to changes in employees' circumstances that could increase incentives for abuse or fraud.
4. The best answer is a) Yes, all systems. Companies should maintain active and up-to-date antivirus protection provided by a reputable vendor. Schedule regular scans of your computer in addition to real-time scanning.
5. The best answer is a) Yes, a formal process where updates are applied at least monthly. Update your software frequently to ensure you have the latest security patches.
6. The best answer is a) No. Limit local administrator privilege on computer systems where possible.
7. The best answer is a) Yes. Use firewalls on your local network to add another layer of protection for all devices that connect through the firewall, such as PCs, smart phones and tablets.
8. The best answer is a) Yes. Intrusion Detection/Prevention Systems (IDS/IPS) are used to monitor network/Internet traffic and report or respond to potential attacks.
9. The best answer is a) Yes, Internet traffic on the system used for "high risk" online baking activities is completely restricted to only sites specifically needed for business functions. Filter web traffic to restrict potentially harmful or unwanted Internet sites from being accessed by computer systems.
10. The best answer is a) Yes. Implementing e-mail SPAM filtering will help eliminate potentially harmful or unwanted e-mails from making it to end users' inboxes.
11. The best answer is a) Yes, and the systems are set to auto-lock after a period of inactivity. Systems should be locked, requiring a password to reconnect when users walk away from their desks to prevent unauthorized access to the system.
12. 12. The best answers are either a) No or b) Yes, but wireless traffic uses industry approved encryption. Wireless waves are easily intercepted by unauthorized individuals.
13. The best answer is a) Yes, behind a locked door. Physically secure critical systems to only allow access to approved employees.
14. The best answer is a) Passwords are securely stored. Passwords should never be left out for unauthorized individuals to gain access.

Connect with us

We are here to help your business succeed. Reach out to any member of our team to find out how we can help your business save time and money .

Click Here and we'll reach out to you.

Products & Services

Remote Deposit for Business

- Electronically submit your checks for deposit
- Save time and money
- 24-hour deposit capability
- Easy to use
- Reduce the risk of check fraud

Lockbox Processing

- Payments are sent to our processing center for handling
- Reduce mail, processing, check clearing float
- Increase interest income or reduce interest expense
- Improve auditing and record keeping

Online Banking

- View accounts and transfer funds
- Direct Deposit Payroll
- EFT tax payments
- Wire Transfer
- ACH payments and receipts
- Collections

Merchant Services*

- Competitive pricing
- Low monthly fee
- Low equipment cost
- Terminal set-up and training
- Local and friendly customer service
- 24-hour customer service hotline
- Proprietary gift cards
- Check Services

* Merchant Services are subject to approval. Additional fees my apply.

** This Product is not a product of the bank and is not insured or guaranteed by the FDIC

Fraud Protection

ACH Debit Block

- Block all ACH debit transactions for each specified account
- Block ACH debit transactions by type; for example WEB (Web initiated transactions) or TEL (Telephone initiated transactions)
- Block all ACH debits that do not match your approved vendor list

Positive Pay

Positive Pay is an automated fraud detection tool that matches the account number, check number and dollar amount of each check presented for payment against a list of checks previously authorized and issued by your company

Sweep Accounts

Credit Sweep Accounts

Minimize interest expense with an overnight payment to your Line of Credit**

Cash Concentration Accounts

Centrally maximize cash by daily sweeping excess deposits from individual operating accounts

Repurchase Sweep Accounts**

Maximize deposit interest earnings with an overnight Repurchase Agreement