Security Check

Are you doing everything you can to protect your business's livelihood?

Online Transaction Precautions

Daily Diligence

- Ideally, establish a stand-alone PC with a clean hard-drive with the sole function to do online banking and card purchases on secure web sites. The PC should be configured that it may not receive emails nor be able to visit any sites other than authorized secure sites and should not be on the same network as the rest of the organization.
- Through your IT department, limit administrative rights on users' workstations. This will help prevent the inadvertent downloading of malware or other viruses by users.
- Lock the workstation to ensure unauthorized users may not gain admittance to computers when left alone.
- Restart at the end of the day.
- Keep anti-virus and anti-spyware tools continually updated and run regular system scans.
- Review account activity DAILY, and confirm last sign on date on the Business eBanking Welcome page.

Cyber Security

Be sure to check with your insurance provider about cyber security options.

Passwords

- Assign each individual a user name and password.
- Common passwords reduce accountability and make it difficult to trace fraudulent activity. Employees who leave the company may continue to have access to tools and services with common passwords.
- Password protect all office computers - and change them frequently.
- Do not share or write down passwords.
- Do not use the “Save Password” feature on login forms.

- Dictionary passwords and “forms” of them are the easiest to hack so try to be creative. For example: fraudsters have programs that will hack 313phant just as quickly as Elephant.
- Pad passwords. Multiple characters before and after a password also add some security - i.e. 000qmb1c5000.

Alerts

Review and set up alerts and notify us immediately if the activity is not recognized.

Text and email alerts allow users to receive alerts whether in the office or out.

An alert is automatically sent:

- when a password is changed
- when a sub-user's role is changed (e.g. when someone is given the approval or administrative role)
- when an e-mail address is changed

Additional alerts may be customized by the user based on the roles that are applicable to their daily functions:

- debit posted
- minimum balance
- stop payment

Dual Control

Dual-control functions provide protection and accountability for your employees in addition to providing an extra layer of fraud protection.

For example, one employee may have authority to prepare ACH files (such as payroll) while another must transmit them.

Use multi-person sign-off for financial activities. More than one person should look at expense reports, payroll, and vendor bills. Sharing accounting duties creates collective responsibility and makes falsifying statements much more difficult.

Terminations

Former employees may be another potential vulnerability. When an employee leaves a company, all computer accounts should be deactivated immediately.

- While online tools are convenient, many may be accessed outside of the office (such as from home or a public computer).
- Lock the user in Business eBanking and notify the Business Service Group at 877-495-6989. ACH and Wire templates are tied to the account not the user that created them, so the templates will not be lost. Scheduled transactions will need to be rescheduled.

BEC and CAT

Business Email Compromise (BEC): Scam that targets both businesses and individuals who use transfer-of-funds requests such as payroll.

Corporate Account Takeover (CAT): Cyber criminals gain control of systems by stealing sensitive employee credentials and information.

Steps that help you AVOID BEC and CAT

1. Require specific documentation for payment requests.
    - Any transfers should have an audit trail of who made the request and why.
2. Double check anything out of the ordinary
    - Don't rely on email or texts for any payment change information. Always call your employee or vendor using a phone number previously used to contact them to ask for verbal verification of the change and request a updated signed copy of the instructions.
3. Mix up your accounting routine
    - Implement segregation of duties between employees for double checks.
4. Get neutral eyes on important documents
    - A secondary reviewer should check the validity of bank statements, reconciliations, and vendor payments each month.

Friendly Reminders from Your Business Banking Partner

Security

- Install, update, maintain and properly use industry standard security products that are appropriate for your business.
- Check your account balances and activity daily and report any suspicious activity immediately by calling 877.495.6989
- Never disclose your passwords and codes to any other person, and take all reasonable actions to maintain their confidentiality.
- Notify us immediately if your phone number, mailing address, or email address that we use to contact you changes.

For more information, refer to the Security Schedule.

Helpful Hints for Money Movement

National Exchange Bank & Trust ACH and Wire Originators are required to use multiple fraud prevention tools that provide additional roadblocks against unauthorized activity. However, these tools are not foolproof systems. The additional suggestions below may reduce your risk of loss should someone obtain access to your PC.

Log In and General Controls

- Do not use account numbers when providing nicknames for the account.
- Limit user access to either Set up an ACH or wire template or to Transmit an ACH or wire transaction. This allows the ability to provide separation of duties within a company.

ACH

- Set daily limits for ACH transactions by user and by account by service: ACH collections, payments, state tax and federal tax.
- Set up Business eBanking alerts to be notified that an ACH template has been modified.
- Establish multiple approvals to transmit an ACH transaction.

Wire

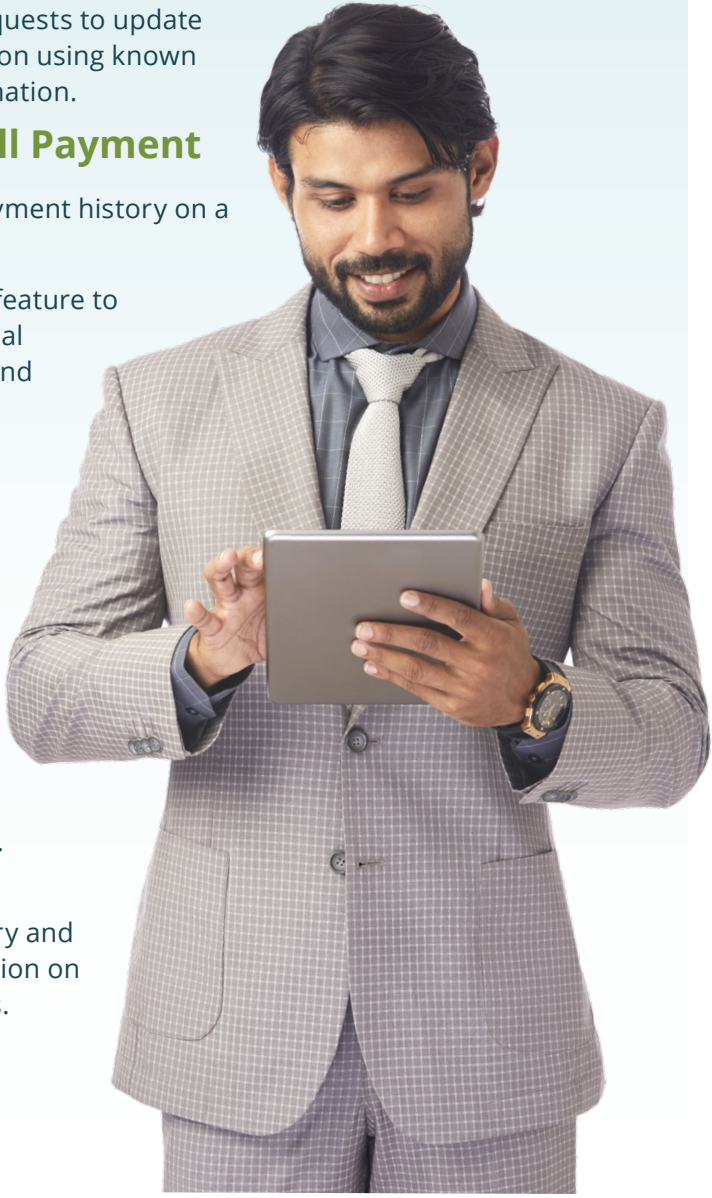
- Set transaction limits for wires by user
- Review wire history on a regular basis.
- Use alerts for wire transfers.
- Create alerts to be generated when a wire template has been modified.
- Validate all requests to update wire information using known contact information.

Business Bill Payment

- Review Bill Payment history on a regular basis.
- Use the audit feature to look for unusual IP addresses and activity.

Funds Transfer

- Set dollar limits on transfers.
- Establish multiple approvals to transmit a funds transfer.
- Review Funds Transfer history and audit information on a regular basis.



Banking & Cash Management

The Business Electronic Banking and Cash Management Agreement between us, National Exchange Bank & Trust, and you, the customer, was entered with agreement to the terms stated by a signature or utilization of our services. Below are some reminders.

The Service

When you use, or you permit any other person(s) to use, any part of the service, you agree to the terms and conditions of the full agreement.

Mobile Banking Service

You agree to allow any authorized person or entity to use the Business Electronic Banking Services through a Mobile Device.

Equipment Access Requirements

You are solely responsible for the prompt adoption of all security patches and other security measures issued or recommended by your software and system providers.

Administrators, Authorized Persons and Service Authorizations

- You must appoint at least one Administrator who will be responsible for creating and maintaining subsequent users for use of Business eBanking, including assigning and revoking access privileges for those Authorized Persons and providing new and subsequent User IDs and passwords and other security devices to those Authorized Persons.
- Administrators have the capability of providing administrative privileges identical to a second Authorized Person, including the ability to create and maintain subsequent Authorized Users assigning and revoking access privileges.

Electronic Mail (“Email”)

Secure electronic communication with us is available inside Business eBanking. You understand and acknowledge that communications transmitted via email outside of the Business eBanking product may not be secure.