Business Online Best Practices

Businesses face increasing challenges in creating a secure online environment. United Savings Bank is committed to helping you address these challenges and as such we recommend implementing a combination of protective measures as part of a comprehensive security plan to minimize risk. The following are a few industry best practices:

-Safeguard your User Name and Password

-Change your password at a minimum every 90 days

-Avoid using automatic login feature that saves your username and password

-Use strong complex passwords

-Check the date and time of your last login every time you login

-Logon to business online only from secure connections, avoid using public WIFI

-Don’t logon to online banking from a public computer

-Logon to online banking by typing in the bank’s website, don’t rely on links pointing you to our website

-Be sure to log out of the business online site when finished

-If applicable, keep your token locked in a secure place

-Review and reconcile your account transactions daily

-Consider establishing a separate account for wire and ach activity

-Set up Notifi alerts in Business online to be alerted of out of band transactions

-Set up dual authentication for wires and ach transactions

-If approving wires or ach transactions, review all the corresponding details before approving. Confirm with the initiator that they created the wire or ach

-Don't share sensitive information via email

-Beware of email and text scams. Don't open an email unless you verified the source.

-Utilize anti-virus, anti-spyware and anti-malware software and keep it up to date

-Keep your operating systems and browser up to date and patched

- Review online banking user ID's and access levels with the bank on a regular basis (ensures correct additions/deletions, etc.)

-Take advantage of transaction limits

-Immediately escalate any suspicious transactions to the financial institution, especially ACH or wire transfers by calling (215)467-4300 or emailing usb@unitedsavingsbank.com.

-Verify use of a secure session (**https** not http) in the browser for all online banking or when submitting or dealing with sensitive information online.

-Consider purchasing cybersecurity and fraudulent fund transfer insurance

-You should perform a risk assessment and controls evaluation periodically

Remember we will never ask you for your logon credentials or personal information over email or via telephone

For more information please visit
https://www.unitedsavingsbank.com/Fraud-and-Security.aspx