# Online Banking Security Awareness

**GenoaBank operates a state-of-the-art Online Banking solution with high-end firewalls and exclusive encryption software security to prevent outside interference.**

## Online Banking Username and Password

Your username and password for your Online Banking accounts should be protected just as you protect other personal confidential information.

- Make your password at least 8 characters long. Longer passwords are harder to crack.
- Use a complex password
- Create passwords that are easy to remember but hard for others to guess.
  - Include numbers, capital letters and symbols
  - Special characters can be used in place of letters. For example use a @ instead of an A.
- Do not share your password with anyone
- Do not write down your username or password
- Do not use the same password for your Online Banking that you use for other websites
- Change your password on a regular basis
- If you access your Online Banking from your phone consider a password for you phone as well
- Avoid accessing Online Banking in cybercafés
- Avoid using an automatic login feature that saves your usernames and passwords
- If you think your password has been compromised, notify the bank immediately

## Online Banking Security Questions

Security questions are just as important as your username and password as they provide an extra level of security for your Online Banking account.

- Select questions that you only know the answers
- The answer should be hard to guess
- Change your questions on a regular basis

## Online Banking General Recommendations

- Never leave the computer unattended while using Online Banking.
- Check your last login date every time you login.
- Never conduct banking transactions while multiple browsers are open on your computer.
- Regularly use the alert systems available to you such as balance alerts and transfer alerts.
- Review historical reporting features on a regular basis to confirm payment and other transaction data.
- Whenever possible, use Bill Pay instead of checks to limit account number dissemination exposure and to obtain better electronic record keeping.
- Do not use account numbers, your social security number, or other account or personal information when creating account nicknames or other titles.
- Review account balances and other detail transactions regularly (preferably daily) to confirm payment and other transaction data. Immediately report any suspicious transactions to GenoaBank.
- Watch for unusual changes in web site appearance or PC behavior when logging in to your online account.

## Internet Browser Security

When using Online Banking there are two ways to make sure your session is secure.

- The presence of https:// in the URL
- The digital certificate represented by a padlock or key in the bottom right hand corner or to the right of the URL text box at the top of the screen. If you double click on the icon it should provide you with information about the organization with which you have entered into a secured session.

## Email Security

Never include personal or account information in an email as it can be intercepted and read by anyone having access to the servers on which it resides. GenoaBank will never ask you to provide any personal or account information via email. Remember, the bank has your account information so there would never be a need to request it from you or ask you to update it.

- Don't open SPAM or attachments from strangers
- Be suspicious of e-mails asking for personal information. If an e-mail claims to be from GenoaBank, call the bank immediately.
- Be selective when providing your email address to third parties
- Never click on links or download an attachment provided in a suspicious e-mail.
- The most common ways to be infected with malware are:
  - Directly downloaded by users who think it is a safe program or file
  - "Drive-by download"- Spyware is installed when a user visits a website
  - Downloaded from an opened and unsolicited e-mail

# Online Banking Security Awareness

## Mobile Device Security

Creating a pass code protects your mobile device and is the first line of security for its content.
Enable the screen lock feature so it automatically locks after a period of inactivity.
After the purchase of a smartphone, learn its features, including the default settings. Turn off features that are not needed to reduce risk, such as Bluetooth.
Avoid clicking on web page or application advertisements. Ads are often a source of malicious software.
When you access a Wi-Fi network that is open to the public, your device can be an easy target for criminals. Only use a network you trust.
If you decide to sell your device or trade it in, make sure you wipe the device (reset it to factory default) to avoid leaving personal data on the device.
Smartphones require updates to run application and firmware. If neglected, it increases the risk of having the device hacked or compromised.
Use the same precautions on your smartphone as you would on your computer when using the Internet.

## PC Security

It is important to use and maintain up to date anti-virus software and install updates as they become available for your operating system.
Use a modern operating system. The most recent Operating Systems (OS) provide substantial security enhancements over earlier operating systems.
Run a scan on your computer with trusted anti-virus software regularly. If the scan detects any suspicious programs or applications, remove them immediately.
Log off when you are done using websites that require a Username and Password.

## What to do if you suspect your account has been compromised

Contact GenoaBank immediately at 1-800-592-2828
Be prepared with all details of the incident, including transaction information, timing, and the manner in which the compromise was identified.
Shut down your web browser and computer, and disconnect your Internet connection and wireless capability.
- If a computer is compromised, any continuing activity or operation could expose additional sensitive information to criminals.
- A computer that is turned off and disconnected from the Internet cannot transmit data to the Internet
- Some malware may exist only in a computer's temporary memory; shutting down the computer might prevent permanent or further infection.
- Change your password and any answers to security questions

## Contact GenoaBank, today!

| | | |
|---|---|---|
| **Elmore** Branch | 352 Rice Street, Elmore OH 43416 | (419) 862-8019 |
| **Genoa** Branch | 801 Main Street, Genoa OH 43430 | (419) 855-8381 |
| **Maumee** Branch | 703 Conant Street, Maumee OH 43537 | (419) 891-0070 |
| **Millbury** Branch | 24950 West State Route 51, Millbury OH 43447 | (419) 836-2351 |
| **Oregon** Branch | 3201 Navarre Avenue, Oregon OH 43616 | (419) 698-1711 |
| **Perrysburg** / **Rossford** Branch | 9920 Old US 20, Rossford OH 43460 | (419) 873-9818 |
| **Sylvania** Branch | 5501 Monroe Street, Sylvania OH 43560 | (419) 841-5501 |
| **Port Clinton** / **Catawba** Branch | 3994 East Harbor Road, Port Clinton, OH 43452 | (419) 734-3994 |