Bank Your Bank of Choice
Owen County State Bank

Internet & Internet Banking Safety Guidelines

Common sense practices can often lower your exposure to risk on the Internet:

- Use spam filters and regularly empty spam folders as they fill.
- Do not click unknown links within emails or verify links received before clicking them.
- Delete questionable emails and don't open unexpected attachments.
- Be skeptical of forms requesting personal info on the Internet.
- Do not participate in Internet transactions where funds are requested to be sent back to the payer.
- Use a password-protected screensaver with an inactivity timer.
- Check accounts often for activity; use Internet Banking Account Alerts for account balance triggers.
- Prohibit the use of "shared" usernames and passwords for online banking systems.
- Always verify use of a secure session (https not http) in the browser for all online banking.
- Avoid using automatic login features that save usernames and passwords for online banking.
- Never leave a computer unattended while using Internet Banking.
- Use anti-virus, anti-malware, anti-spyware software and a firewall.
- Report any suspicious transactions to Owen County State Bank immediately. There is a limited recovery window for these transactions and immediate escalation may prevent further loss by the customer.

Wireless Security

Wireless Internet access can offer convenience and mobility. But there are steps you should take to protect your wireless network and the computers within it.

- Do not use public "hot spots" to access Internet Banking or other secure sites, or to make online transactions. Public hot spots are inherently insecure and provide an environment for others to intercept your transmitted data.
- Change your router/access point's default password - Most network devices, including wireless access points, are pre-configured with default administrator passwords to simplify setup. These default passwords are easily found online, offering no protection.
- Changing default passwords makes it harder for others to take control of the device.
- Restrict access - Only allow authorized users to access your network. Each piece of hardware connected to a network has a MAC (media access control) address. You can restrict or allow access to your network by filtering MAC addresses. Consult your user documentation to get specific information about enabling these features.
- Encrypt the data on your network - WPA (Wi-Fi Protected Access) encrypts information on wireless devices. WEP also offers encryption but is far easier to compromise than WPA. Data encryption prevents others from easily viewing the data within your network.
- Protect your SSID (wireless network name) - To avoid outsiders easily accessing your network, prevent your access point from broadcasting its SSID. It is also recommended to change the manufacturer's default SSID to make it more difficult to guess.
- Turn off your wireless network when you know you won't use it.

Password Strength

Keys to password strength: length and complexity. Choose a strong password you can remember, keeping in mind that:

- An ideal password is long (10 or more characters) and has letters, punctuation, symbols, and numbers.
- The greater the variety of characters in your password, the better.

Avoid creating passwords that include:

- Dictionary words in any language, including words spelled backwards, common misspellings, and abbreviations.
- Sequences or repeated characters. , such as 12345678, 22222222, qwerty, or zyxwvut.
- Personal information, such as your name, birthday, driver's license, or similar information.

Password Security

Maintaining strong passwords and keeping them secure is one of the best ways to keep you and your information safe.

- Never provide your password over e-mail or in response to an e-mail request: Internet "phishing" scams use fraudulent e-mail messages to entice you to reveal your user names and passwords, steal your identity, and more.
- Do not type passwords on computers that you do not control: Computers such as those in Internet cafes, computer labs, kiosk systems, conferences, and airport lounges should be considered unsafe for any personal use other than anonymous Internet browsing. Cyber criminals can purchase keystroke logging devices which gather information typed on a computer, including passwords. Don't reveal passwords to others
- Keep your passwords hidden from friends or family members who could pass them on to other, less trustworthy individuals.
- Protect any recorded passwords: Don't store passwords on a file in your computer, because criminals will look there first.
- Use more than one password: Use different passwords for different Web sites and services.

To lower your risk of spyware and malware infections:

- Update your operating system and Web browser software, and set your browser security high enough to detect unauthorized downloads.
- Use anti-virus and anti-spyware software, as well as a firewall if possible, and update them all regularly.
- Download free software only from sites you know and trust. Enticing free software downloads frequently bundle other software, including malware.
- Don't click on links inside pop-ups.
- Don't click on links in spam or pop-ups that claim to offer anti-spyware software; you may unintentionally be installing spyware instead.
- Know who you're dealing with. In any electronic transaction, including those with a business, independently confirm the other party's name, street address, and telephone number. Don’t do business with anyone that will not provide this information.
- Resist the urge to enter online lotteries, both foreign and domestic. These solicitations are often phony and illegal.
- Delete requests that claim to be from foreign nationals asking you to help transfer their money through your bank account. They're fraudulent.

- Ignore unsolicited emails that request your money, credit card or account numbers, or other personal information.
- If you are selling something over the Internet, don't accept a potential buyer's offer to send you a check for more than the purchase price, no matter how tempting the plea or convincing the story. End the transaction immediately if someone insists that you wire back or send back part of the funds.
- Take your time. Resist any urge to "act now" despite the offer and the terms. Once you turn over your money, you may never get it back.
- Read the small print. Get all promises in writing and review them carefully before you make a payment or sign a contract.
- Never pay for a "free" gift. Disregard any offer that asks you to pay for a gift or prize. If it's free or a gift, you shouldn't have to pay for it. Free means free.
- Protect your personal information. Share credit card or other personal information only when you're buying from a company you know and trust.

These tips and others are available from **www.staysafeonline.org** sponsored by the National Cyber Security Alliance, **www.ftc.gov** maintained by the Federal Trade Commission, and **www.fraud.org**, sponsored by the National Consumer League.