Security Tips

Keeping your personal, private information secure.

Be cautious when sharing your personal information. Peoples Bank will never ask for your social security number, user ID, account number, or password via email or phone when we call you. Never provide your social security number, user ID, account number, or password via email or by phone to businesses or persons you do not know. Never authorize someone else to "use" your account to negotiate checks, make deposits, or receive or send wire transfers.

Keep your contact information current. Correct email addresses, cell phone numbers, and mailing addresses ensure we can contact you regarding your account, including notification and alert features.

Be cautious of suspicious emails or phone calls. Be skeptical of unsolicited emails and calls. Legitimate companies will never contact you via phone or email with a request to provide your social security number, username, password, or account information. Even if it is a company you do business with, if you did not expect the request or if the request isn't logical, you should verify the company sent it before responding. Never call back a number provided on the solicitation itself. Use a known public phone number or email contact.

Use online statements to protect from mail fraud. Protect your account information by signing up for online statements. Electronic delivery of statements eliminates the risk of mail theft. Online statements may be reviewed, printed, or downloaded through your secure Peoples Online Banking account.

Notifications and Alerts. Use online banking alerts to monitor transactions and online banking activity. Within online banking, you can enroll in email and text alerts that will generate notifications to alert you of transaction activity or balance information according to criteria you have established.

Keep your passwords, personal identification numbers (PINs), and account codes secret. Your User ID and password are the most critical layer in online banking security. Use truly unique passwords that only you know. Longer passwords that include special characters and numbers are more secure. Avoid names, dates, or common phrases that might be guessed.

Use the passcode lock on your smartphone and other devices. The more security layers, the more difficult it is for thieves to access your information if your device is lost or stolen.

Peoples Bank

peoplesbank-wa.com/online-security

Security Tips continued

Keep your systems up to date. Install updates and use antivirus software where available for all systems that access financial information. Timely installation of updates is important to safeguard your personal and financial information.

Traveling with your card: If you intend to travel out of state or internationally and you wish to have access to your Peoples Bank account during that time, please contact customer service (1-800-584-8859) at least 48-hours prior to departure to have the restriction lifted.

For Business Customers. Develop a good employee education program that covers current scams and fraud. Establish unique usernames and passwords for your staff. Limit access to functionality that is necessary for their work. Utilize transaction limits, tokens or out-of-band approval, and dual control for ACH and wire transactions.

Reporting Security Concerns. If you suspect that you have been the victim of fraud or identity theft, see unauthorized transactions, believe that your online banking credentials have been compromised, have a lost or stolen card, wallet or purse, or have received suspicious emails or checks for deposit, please contact us immediately at 1-800-584-8859.

Additional Resources:

Identity Theft:
https://www.identitytheft.gov/

Stay Safe Online:
https://staysafeonline.org/stay-safe-online/

Federal Trade Commission:
https://www.consumer.gov

Peoples Bank Security Center:
https://www.peoplesbank-wa.com/online-security

Peoples Bank