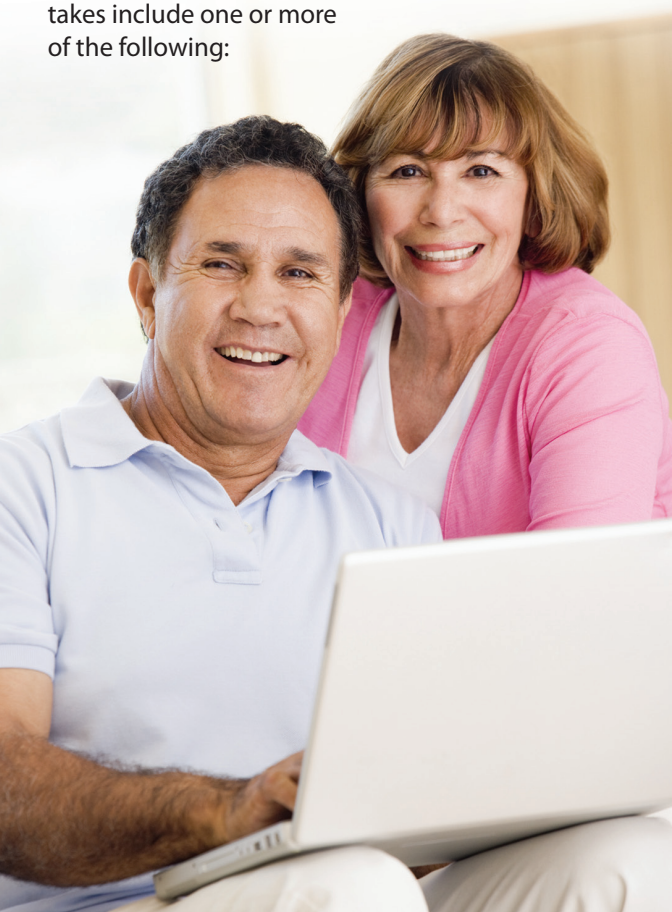
Safe & Secure

ONLINE BANKING

- ☑ **Understanding** the threats
- ☑ **Protecting** against account fraud and identity theft
- ☑ **Securing** your Internet transcations

Making Online Banking Safe & Secure

While you're at home on the internet accessing online banking, you want to be assured that effective safeguards are in place to make your visit safe, secure, and reliable. When you use online banking to visit Century Savings Bank, whether it's to learn about rates, to review your accounts or to pay your bills, you are entering a secure area. Measures the bank takes include one or more of the following:



❖ PASSWORD PROTECTION AND PIN

Your password and PIN (personal identification number) are the first line of defense, and are your unique identifier. Be sure not to share them with anyone–most frauds involving hijacked accounts originate with someone the victim knows.

❖ MULTI-FACTOR AUTHENTICATION

Multifactor Authentication (MFA) is a security system in which more than one form of authentication is implemented to verify the legitimacy of a transaction.

❖ ENCRYPTION

Your transactions and personal information are secured by encryption software that converts the information into code that is readable by only you and Century Savings Bank.

❖ PRIVACY POLICIES

Bank privacy policies maintain strict physical, electronic, and procedural safeguards that comply and meet with federal standards to guard your nonpublic personal information.

Using Online Banking

Whether you are conducting online financial transactions over the Internet or simply "surfing," some easily implemented precautions can help safeguard your personal information from identity theft and account fraud. The following are steps YOU can take:

❖ PASSWORDS

Security begins with a strong password, which only you, the user, knows. Your computer passwords should be complicated, even if it just means adding a few extra numbers or letters. You should also consider changing your password every 30 to 60 days or so.

❖ ANTI-VIRUS PROTECTION

Make sure the anti-virus software on your computer is current and scans your email as it is received. This simple step is critical to your personal safety and security when online.

❖ EMAIL COMMUNICATION

Email is generally not encrypted so be wary of sending any sensitive information such as account numbers or other personal information in this way. If you receive an unscheduled or unsolicited email claiming to be from our bank be cautious – take the time to give us a call and make sure the email was sent from Century.

❖ SIGNING OFF

Always log off by following the bank's secured area exit procedures to ensure the protection of your personal information.

❖ BE AWARE

Internet criminals are trying to get your personal information – and they employ ingenious methods. Don't respond to any unusual requests for personal information – when you opened your bank accounts you already gave it. When in doubt, give us a call.

Identifying the Most Common Online Threats

You can best protect yourself by understanding what criminals are doing over the Internet. Most electronic fraud falls under one of three categories.

❖ PHISHING

As scam artists become more sophisticated, so do their phishing e-mail messages and pop-up windows. They often include official-looking logos from real organizations to lure you to a copycat web site. These copycat sites are also called "spoofed" web sites. Once you're at one of these spoofed sites, you might unwittingly send personal information to the con artists. If you receive a suspicious email, delete the message and call your bank to inform them of the email.

❖ PHARMING

Also called "domain spoofing," this crime intercepts internet traffic and re-routes it to a fraudulent site. Once there, the victim is asked to enter personal information, just as with phishing. It is different than phishing in that the attacker does not have to rely on having the user click a link in an email to deceive the user.

❖ MALWARE

This is software designed to hijack or damage a computer system without the user's knowledge. The intent may be to steal your identity or track your activities. Examples of malware (malicious software) include computer viruses, worms, Trojan horses, spyware, and adware.

Want to know more?

Stop by your bank today to learn more about online banking and the security measures that are in place for your protection. Or contact any of these financial industry regulators:

Federal Deposit Insurance Corporation
www.fdic.gov

Board of Governors of the Federal Reserve System
www.federalreserve.gov

Office of the Comptroller of the Currency
www.occ.treas.gov

Office of Thrift Supervisor
www.ots.treas.gov

Federal Trade Commission
www.ftc.gov

CENTURY
SAVINGS BANK
Since 1865
community banking *plus*

www.**centurysb**.com

MEMBER FDIC

EQUAL HOUSING LENDER

02/2014