

Your Security

Your Security is important to us at Century Bank. We want to provide you with tools and resources that will assist you in preventing identity theft. **Century Bank will never require customers to send personal information via email or pop-up windows.**

Identity Theft

By understanding exactly what identity theft is, how it happens, and how it affects you, you will

be better able to prevent and, if necessary, resolve identity theft.

In general identity theft is more extensive than fraud, which is usually limited to an isolated

attempt to steal money from an existing account. Fraud and identity theft can be easily confused.

What is Identity Theft?

Identity theft occurs when someone illegally obtains your personal information, such as your

social security number, bank account number, or other identification, and uses it repeatedly to

open new accounts or initiate transactions in your name. For example, someone might do a

combination of the following: open new credit cards, open new bank accounts, forge checks,

and even apply for loans using your name and personal information. This can cause financial

loss and damage your credit, which can lead to a lengthy resolution process.

Keep in mind however, that even if you think your security has been compromised it does not

automatically mean that you are a victim of identity theft. It might be an incorrect entry or an

isolated incident of theft from your account that is quickly resolved by calling Century Bank at

541-684-0515.

How does identity theft happen?

Identity theft is portrayed as a high-tech crime affecting only those people who shop, communicate, or do business online. However, while thieves can obtain personal information

via online methods, the majority of identity theft occurs offline. Stealing wallets and purses,

intercepting or rerouting your mail, and rummaging through your garbage are some of the

common tactics that thieves can use to obtain personal information. The good news is that the

more information you have on identity theft the better your defense.

What is "Phishing"?

Phishing (pronounced "fishing") is a form of online scam where "phishers" attempt to gain customer account information such as user names, passwords, PINs (personal identification

numbers), or social security numbers. This is accomplished by creating official looking emails

with pop-ups or links that appear to be from your bank, online retailer, or government agency.

These deceptive communications are the tools the “phishers” use to attempt to gain your confidential information.

Page 1 of 6

How does “Phishing” work?

These phony emails often use phrases such as “your account may have been compromised”,

“your account is in violation”, “we need you to verify your account information” and other variations. These emails will then usually offer a link where you can access your account to

prevent adverse actions such as account closure or a freeze on an account’s assets.

These

links will then connect you to a site that will often times look identical to the business site the

email refers to. These sites however, are forgeries created to trick users into logging into the

sites with their genuine user ID and password. Once the “phishers” have obtained this information they can then go to the real website and transfer, withdraw, or redirect the funds to

another location. Then when the customer logs into their account again (on the real business

website) they are surprised to find all of their assets are gone. In addition to loss of funds, there

can also be adverse credit affects which may take weeks or months to resolve.

How can I protect myself from “Phishing” attacks?

The most important thing to remember is that no reputable business will send you an email

requesting your personal account information. Any email you receive asking for this information

should be considered phony and brought to the attention of the business being “phished”.

Another way to further protect yourself is to keep your Operating System and Internet Browser

software up to date. “Phishers” often use software vulnerabilities to further mask their deception

on their fake websites.

Also, antivirus software can often detect methods used by “phishers” attempting to steal your

information. But it is imperative that your antivirus software be updated as frequently as possible.

Finally, if you are unsure as to whether or not an email or message is legitimate, call the company directly. That way you can be sure that you are speaking with a representative of that

company and that your personal information will not be compromised.

What is “Spoofing”?

Spoofing is pretending to be something it is not, on the Internet, usually an e-mail or a Web site.

What if you downloaded a Virus or “Trojan Horse”?

Some phishing attacks use viruses and/or “Trojan Horses” to install programs called “Key

logger” on your computer. These programs capture and send out any information that you type to the phisher, including credit card numbers, user names and passwords, Social Security numbers etc. If this happens, it is likely you may not be aware of it until you notice unusual transactions on your account.

To minimize this risk, you should:

- Install and/or update anti-virus and personal firewall software. (several products are available online or through computer retail stores.)
- Update your anti-virus programs often and all virus definitions and run a full scan.
- If your system appears to have been compromised, repair it and then change your password again, since you may have transmitted the new one to the hacker.

Page 2 of 6

- Check your other accounts. eBay account, PayPal, your e-mail ISP, online Bank accounts, online trading accounts and other e-commerce accounts, and everything else for which you use online passwords, to ensure they remain secure and have not been compromised by unauthorized access.

What is “Skimming”?

Thieves steal credit/debit card numbers by using a special storage device when processing your card.

ATM / Debit Card Transaction Monitoring – We may be calling you

To protect your account, we monitor your ATM & debit card transactions for potentially fraudulent activity which may include a sudden change in locale (such as when a US issued card is used unexpectedly overseas), a sudden string of costly purchases, or any pattern associated with new fraud trends around the world.

If we suspect fraudulent ATM or debit card use, we’ll be calling you to validate the legitimacy of your transactions. Your participation in responding to our call is critical to prevent potential risk and avoid restrictions we may place on the use of your card.

- Our automated call will ask you to verify recent transaction activity on your card.
- You will be able to respond via your touchtone keypad.
- You will also be provided with a toll free number to call should you have additional questions.

Our goal, quite simply, is to minimize your exposure to risk and the impact of any fraud. To

ensure we can continue to reach you when ever potential fraud is detected, please keep us

informed of your correct phone number and address at all times.

In the meantime, please be diligent in monitoring transaction activity on your account and

contact us immediately if you identify any fraudulent transactions. Here are some additional tips

on protecting your self from debit card fraud:

Protect yourself

Unless absolutely required for legitimate business purpose, avoid giving out your:

- Address & ZIP code

- Phone number
- Date of Birth
- Social Security number
- Card or account number
- Card expiration date

Your PIN is private; never give it out

In stores and at ATM's, always cover your card and PIN, and watch for:

- Cell phone cameras, mirrors, or other tools used to view cards and PINs
- People watching your transactions
- Cashiers taking your card out of sight; take it to the register yourself
- Any unusual activity at ATMs; if you feel uncomfortable, go to another ATM

Page 3 of 6

Online, you should never respond to unsolicited emails that:

- Ask you to verify your card or account number; such emails are not sent by legitimate businesses
- Link to websites; such sites can look legitimate but may collect data or put spyware on your computer

More tips on protecting yourself

Do not open or respond to online solicitations for personal information. ***Century Bank will never require customers to send personal information via e-mail or pop-up windows.***

Carry only necessary identification. In particular, do not carry your social security card.

When a social security number is requested to sign up for a service, confirm that it is actually needed rather than some other identifier.

Make photocopies of all the information you carry daily and store them in a secure location like a safety deposit box.

Shred financial or personal documents before discarding. Most fraud and identity theft incidences happen as a result of mail and garbage theft.

Checking your account balances and transactions online can help you regularly monitor

your account activity and more quickly detect any fraudulent transactions.

Do not use an obvious password like your birth date, your mother's maiden name, or the

last four digits of your Social Security number.

Always put outgoing mail in a U.S. Postal Service mailbox, which is more secure than your home mailbox.

Collect your mail promptly each day.

How can I detect fraud?

Be aware of bills that do not arrive as expected.

Receipt of unexpected credit cards or account statements.

Denial of credit for no apparent reason.

Calls or letters about purchases you did not make.

Monitor your accounts online for any unauthorized transactions.

What do I do if I am a Victim?

If you have given out your credit or debit card information

- Report the incident to the card issuer as quickly as possible.
- Report using toll free numbers and 24 hour service that many companies have established to deal with such emergencies.
- Request your card issuer close your compromised account number and reissue you a new card with a different number
- Monitor your account activity and review account statements carefully after the information loss.
- If any unauthorized charges appear, call the card issuer immediately and follow up with a hard copy letter via a traditional delivery service such as U.S. Postal Service describing each questionable charge (keep a copy for yourself).

Credit or Debit Card Loss or Fraudulent Transactions

Page 4 of 6

As a consumer you are protected by Federal law and by many card protection programs if you exercise reasonable care and report any unauthorized transactions promptly.

- It is very important that you continually monitor your monthly statements to identify any unauthorized transactions.
- If you notice fraudulent activity, promptly notify your financial institution or card issuer to report it.

If you have given out your Bank Account Information

- Report theft of this information to the bank as quickly as possible.
- Request your bank close the compromised account and reopen a like account with a different number.

If you have given out your personal identification information

If you believe you have given out personal information such as your name, address, and social

security number to someone who may use it for fraud:

Contact the three major credit reporting agencies – Experian, Equifax and TransUnion and do the following:

- Request a free copy of your credit report to check whether any accounts were opened without your consent.
- Request that the agencies place a fraud alert and a victims statement in your file.
- Request that the agencies remove inquiries and or fraudulent accounts stemming from the theft

Major Credit Bureaus

Equifax – www.equifax.com

- To order your report call: 800-685-1111 or write: P.O. Box 740241 Atlanta, GA 30374-0241
- To report fraud call: 800-525-6285 and write: P.O. Box 740241, Atlanta, GA 30374-0241
- Hearing impaired call 800-255-0056 and ask the operator to call the Auto Disclosure Line at 800-685-1111 to request a copy of your report

Experian – www.experian.com

- To order your report, call: 888-EXPERIAN (397-3742) or write: P.O. Box 2002, Allen

TX 75013

To report fraud, call: 888-EXPERIAN (397-3742) TDD: 877-553-7803 and write: P.O. Box 9530, Allen TX 75013

TransUnion – www.transunion.com

To order your report, call: 800-888-4213 or write: P.O. Box 1000, Chester, PA 19022

To report fraud, call: 800-680-7289 TDD: 877-553-7803 and write: Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92634

Additional Actions to Take if you believe that you are a victim of identity theft:

Page 5 of 6

If bank accounts were set up without your consent close them.

Contact your local police department to file a criminal report.

Contact the Social Security Administration's Fraud Hotline to report the unauthorized use

of your personal identification information.

Contact the department of Motor Vehicles to see whether an unauthorized driver's license number has been issued in your name and to notify them of the identity theft.

Notify the passport office to be on the lookout for anyone ordering a passport in your name.

File a complaint with the Federal Trade Commission.

Online at <http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/filing-a-report.html>

Or call the FTC's Identity Theft Hotline, toll free at 1-877-IDTHEFT (438-4338); TTY: 1-866-653-4261

Or write: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Ave, NW Washington DC 20580

Ask for a free copy of "Take Charge: Fighting back Against Identity Theft: a guide that will help you recover from your theft – and guard against it in the future

File a complaint with the Internet Crime Complaint center (IC3) by visiting their web side: www.ic3.gov. IC3 is a partnership between the Federal Bureau of Investigation (FBI) and the National White Collar Crime Center (NW3C), with a mission to address fraud committed over the Internet. For victims of Internet fraud, the Center provides a convenient and easy to use reporting mechanism that alerts authorities of a suspected criminal or civil violation.

Document the names and phone numbers of everyone you speak to regarding the incident. Follow up your phone calls with letters. Keep copies of all correspondence.

Identity Theft Resources

- <http://www.identity-theft-help.us/>
- <http://www.identitytheft.org>
- www.justice.gov/criminal/fraud/websites/idtheft.html
- <http://www.ic3.gov>
- www.ftc.gov/bcp/edu/microsites/idtheft/

Page 6 of 6