

# Verifying Your Identity

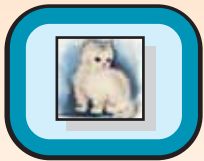
Added Security for Banking Online  
from  
**Blackhawk Bank**  
MEMBER FDIC



The protection of your personal and financial information is our top priority. As technology develops, we're committed to bringing you the most up-to-date security methods to help protect you and your money from identity theft.



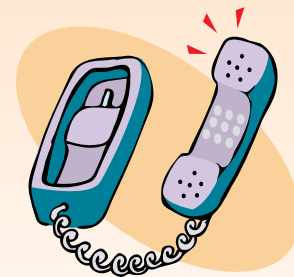
This added security, called Multi-Factor Authentication, adds more ways to verify that you are logged onto the **GENUINE** Blackhawk Bank website, and it's **YOU** accessing your accounts.



In the near future, when you log in, you will be asked to select a picture that will guarantee that you're on Blackhawk Bank's website, not an imposter site. From then on, you'll see this unique photo every time you log in to NetTeller.



You will also be required to provide unique answers to specific questions. Afterward, when you log into NetTeller, if our technology doesn't recognize the computer being used, your log-in location, or if you're attempting to conduct a transaction that requires more authorization, you will be asked to provide those unique answers.



*If you have any questions,  
please call 800.209.2616  
and ask to speak with a  
Customer Support Specialist.*

## Awareness - Your Best Defense Against Identity Theft

These are threats to be aware of, and reasons why Blackhawk Bank is adding extra security for banking online. Share this information with your kids, parents and friends.

**Phishing** - lures you into a fake website (one that looks like a trusted site) and tricks you into providing personal information, such as account numbers and passwords. Never share this information in an email.

**Pharming** - similar to Phishing, Pharming seeks to obtain personal information by directing you to a copycat website where your information is stolen, usually from a legitimate looking form. (Look for that unique photo you selected to guarantee you're on Blackhawk Bank's NetTeller.)

**Malware** - short for malicious software, often included in spam emails that can take control of your computer without your knowledge and forward to fraudsters personal information such as IDs, passwords, account numbers and PINs.

You can make your computer safer by installing and regularly updating your

- Anti-virus software
- Anti-malware programs
- Firewalls on your computer
- Operating system patches and updates

## Tips for Protecting Yourself

Although there's no guaranteed way to avoid becoming a victim of Identity Theft, instituting these protective measures can greatly minimize your exposure:

- Carefully review all account statements regularly. Notify us if you see any discrepancies.
- Do not provide any information to a third party unless you're confident of the purpose and feel secure that the information will not be misused. Never give information by email, or to someone that calls you asking for account numbers, PINs or passwords.
- Notify us immediately if you suspect your accounts have been compromised or if you've lost any cards or checks.
- Keep a list of account numbers in a secure, confidential place in case you experience problems with lost cards or the theft of checks.
- Place only minimal information on the top of your checks - initials, last name, and address.
- Check your credit report at least twice a year. You're entitled to one free credit report from each of the three major credit reporting agencies each

year. Contact them at [www.annualcreditreport.com](http://www.annualcreditreport.com) or call 1.877.322.8228.

- Shred or destroy any documents that contain personal information before putting them in the garbage.
- Remove mail from your mailbox promptly; refrain from putting outgoing mail in your box for your carrier to pick up. Take it to a secure USPS drop-box.
- Do not write PINs on plastic cards in your wallet or purse.
- Ask service providers to stop using your Social Security Number as an identifier. Ask for a different ID number.
- Review your Personal Earnings and Benefits Statement from the Social Security Administration annually.
- Report suspicious activity to a law enforcement agency and your financial institution.

**Be assured that Blackhawk Bank takes the protection of your personal and financial information very seriously. Thank you for your trust and confidence.**