Online Banking Security

Blackhawk Bank is dedicated to helping you keep your online banking experience safe and secure. Education is key to your understanding of the safeguards that should be employed to help you reduce your risk for fraudulent activity when banking online. Blackhawk Bank utilizes state of the art encryption software, multi-factor authentication and secure email to help protect you against fraudulent activity. In addition, there are precautions that you should take to protect your PC from viruses and malware.

What you should do:

Ideally, use a **dedicated computer for online banking ONLY** and a separate computer for email, surfing the Internet and online shopping. This is the best way to prevent the possibility of malicious software infecting the computer you use for online banking. Computer technology advances (e.g. 'Notebook' laptops) have made the purchase of a dedicated computer an inexpensive means of protection.

Learn ways to protect your mobile device:
www.blackhawkbank.com/consumer-safety

If you choose not to use a dedicated computer:

Avoid Spyware. The best way to protect your computer from spyware is to install an anti-spyware program that monitors the activity of software on your computer. Like a virus scanner, anti-spyware software detects and attempts to remove malicious applications from your computer. Spyware infects computers when the user interacts with a malicious source on the Internet.

Use software that scans for viruses.

Note: There are a number of malicious programs that purport to be anti-virus and anti-spyware applications. When installing anti-virus and anti-spyware be sure they are legal licensed versions of the software.

The following rules will help keep your computer safe:

- Do not respond to unsolicited (spam) email.
- Do not click on a link within an unsolicited email.
- Be cautious of email claiming to contain pictures in attached files as the files may contain viruses. Only open attachments from known senders. Virus-scan the attachments if possible.
- Contact the actual business that supposedly sent the email to verify if the email is legitimate.
- Avoid visiting websites that contain questionable content, including sites that offer illegal music, movie and software downloads.
- Pay attention to the Google Results page. Google identifies sites that may contain malicious content. Avoid clicking links that have been identified as such.
- To protect your privacy and help prevent unauthorized use of online banking you should *always 'Exit'* secure websites to completely log-out. *Do not simply click the X to close your Internet session.*
- Monitor your accounts and review your transactions regularly. Should you see suspicious activity, report it immediately.
- Use encryption software on laptop computers.
- Familiarize yourself with the Security Settings on your PC.
- Educate all online banking users in your home about the risks and safeguards.

Tips for Creating and Using Safe Passwords

In addition to the suggestions offered above, follow these NetTeller rules for creating and using strong passwords FOR YOUR ACCOUNTS:

- Must be 8-20 characters with at least 1 letter and 1 number
- Must contain at least 1 of these characters: + _ % @ ! $ ~
- Must contain at least 1 upper and 1 lower case letter
- Must not match or contain your user ID
- When you change your Password in the future, it cannot match one of your previous 4 passwords.
- Make your password easy to type quickly. This will make it harder for someone looking over your shoulder to steal it.
- ***Here are some other password tips:*** Consider using a phrase or a song title as a password. For example, "Somewhere Over the Rainbow" becomes "Sw0tR8nBO" or "Smells Like Teen Spirit" becomes "sMlk10nspT". Make your passwords long and complex, so they are hard to crack. Place numbers and punctuation marks randomly in your passwords.

Using your password safely:

- Create different passwords for different accounts and applications. That way, if one account is breached, your other accounts won't be put at risk too.
- Never use your NetTeller password for online shopping sites or free email accounts (Hotmail, Yahoo!, Gmail).
- Change your passwords regularly, about every 90 days.
- Don't share your password with anyone else. Once it's out of your control, so is your security.
- Never enable the "Save Password" option, even if prompted to do so. Pre-saved passwords make it easy for anyone else using your computer to access your accounts.
- Never walk away from a shared computer without logging off. This will ensure no other users can access your accounts.
- Don't use sample passwords given on different websites, including the samples listed above.

How Passwords are stolen:

When you are creating a strong password, it can help to know the tactics hackers use to steal them. Here are some of the most frequently used techniques:

- **Guessing.** Programs designed to guess a user's password are common. They often use personal information found online—such as names, birth dates, names of friends or significant others, pet names or license plate numbers—as a starting point. These programs can even search for a word spelled backwards.

TIP: *It's best to steer clear of any personally identifying information when creating a password.*

- **Dictionary-based attacks.** Programs and software also exist that run every word in a dictionary or word list against a user name in hopes of finding a perfect match.

  TIP: *Staying away from actual words, even in a foreign language, is recommended.*

- **"Brute Force" attacks.** By trying every conceivable combination of key strokes in tandem with a user name, brute force attacks often discover the correct password. Programs can execute a brute force attack very quickly.

  TIP: *The best way to beat such an attack is with a long, complex password that uses upper and lower case letters, numbers, special characters and punctuation marks.*

- **Phishing.** Phishing scams usually try to hook you with an urgent IM or email message designed to alarm or excite you into responding. These messages often appear to be from a friend, bank or other legitimate source directing you to phony websites designed to trick you into providing personal information, such as your user name and password.

  TIP: *Best advice is don't click a link in any suspicious emails, and don't provide your information unless you trust the source.*

- **"Shoulder surfing."** Passwords are not always stolen online. A hacker who is lurking around in a computer lab, cybercafé or library may be there for the express purpose of watching you enter your user name and password into a computer.

  TIP: *Try to enter your passwords quickly, without looking at the keyboard, as a defense against this type of theft.*

- **Keystroke logging** (often called keylogging) is the practice of tracking (or logging) the keys struck on a keyboard, typically in a covert manner so that the person using the keyboard is unaware that their actions are being monitored. There are numerous keylogging methods, ranging from hardware and software-based to electromagnetic and acoustic analysis. We recommend not using public computers as they may contain this type of malicious software.

  Most antivirus companies have added known keyloggers to their databases, making protecting against keyloggers no different than protecting against other types of malicious programs: install an antivirus product and keep its database up to date. However, since most antivirus products classify keyloggers as potentially malicious, or potentially undesirable programs, users should ensure that their antivirus product will, with default settings, detect this type of malware. If not, then the product should be configured accordingly, to ensure protection against most common keyloggers.

To stay informed about fraud, go to:
www.blackhawkbank.com/consumer-safety

Also you can go to **Online & Mobile,** then to the drop-down menu; choose **Online Banking Security**. The page contains a link to the FBI's website and offers an abundance of information regarding documented fraudulent schemes and activities. The site also offers you the opportunity to sign up and receive email updates whenever new scams and warnings are posted to the site.

Contact Us

If it's after hours and you have an urgent inquiry or problem, leave your name and a phone number where you can be reached. A Client Services Representative will contact you as soon as possible the next business day.

Client Services:
608.364.8924, or Toll-free 866.771.8924
8:00 AM - 6:00 PM Monday - Friday
8:30 AM - 12:30 PM Saturdays

Email:
nethelp@blackhawkbank.com
Please do not send any personal financial information to us via unsecure email

Banking Centers:
Toll-free 800.209.2616
400 Broad Street, Beloit, WI • 608.364.8911
2200 Cranston Road, Beloit, WI • 608.364.8900
2525 Milton Avenue, Janesville WI • 608.314.0084
5506 Clayton Circle, Roscoe, IL • 815.623.3323
9609 Forest Hills Road, Machesney Park, IL • 815.639.0777
2475 N. Perryville Road, Rockford, IL • 815.636.4371
3101 11th Street, Rockford, IL • 815.986.7174
2141 N. State Street, Belvidere, IL • 815.544.0777

US Mail:
Blackhawk Bank • PO Box 719 • Beloit, WI 53512-0719

Bank-by-Phone 24/7:
Toll-free 888.769.2600

To Report a Lost or Stolen Debit MasterCard:

Login to NetTeller > Click **Options** > Click **ATM/Debit Card** > Check the box under **Lost/Stolen** > Click **Submit**. When the next screen appears, click **Submit** once again and the Card will be closed immediately.

Other ways to report a Lost or Stolen Debit MasterCard:

- Use your Blackhawk Bank App
- Call Bank-by-Phone: 888.769.2600
- During business hours call Client Services:
  608.364.8924 / Toll-free 866.771.8924
- After hours call 866.546.8273

Replacement Card

Come to any Blackhawk Bank office during regular hours to get a new Instant Issue Debit MasterCard and PIN. Instant Issue puts a new Card into your hands right away.

OR

Call Client Services @ 866.771.8924 to order a new Card and PIN. It may take up to 10 days to receive your Card and PIN, mailed separately.

Please note: You cannot re-activate a card once you report it as Lost or Stolen. You must get a new card. There is a $10.00 Fee for Lost or Stolen replacement Debit Cards.