

Online Banking Security:

Deter, Defend & Detect.

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.

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 resource 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 Web sites 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 click-



ing 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 guidelines for creating and using strong passwords:

- Use BOTH upper- and lower-case letters.
- Place numbers and punctuation marks randomly in your password.
- Make your password long and complex, so it is hard to crack. Between 8 to 20 characters long is recommended. Use one or more of these special characters: ! @ # \$ % * () - + = , < > : ; " ' `
- To help you easily remember your password, 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 "sMll10nspT."
- Make your password easy to type quickly. This will make it harder for someone looking over your shoulder to steal it.

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 e-mail accounts (Hotmail, Yahoo!, Gmail).
- Change your passwords regularly, about every six months.
- 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.

continued on back

continued from front

- 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 Web sites, 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 e-mail 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 Web sites 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 e-mails, 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.

In a continuing effort to keep you informed about fraud, go to www.blackhawkbank.com and navigate to **Online Banking**, then to the drop-down menu and choose **Security Policy**. 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.



608.364.8911 | 800.209.2616

www.blackhawkbank.com

Bank-by-Phone: 608.364.4534 or 888.769.2600