

Online Banking the Safe Way

Keep Yourself Safe!

◆ Understanding the Risks

As the Internet continues to become a more popular avenue for business and banking transactions, attempts to gain access to your sensitive information also continue to increase and have become more sophisticated. This evolving threat environment requires complex identification procedures (multi-factor authentication) and the use of different controls throughout the transaction process (layered security approach) to combat these threats.

Harvest Bank continues to maintain a low risk posture in allowing only in-bank transfers from our online banking system. In addition, our online banking system employs multi-factor authentication - requiring a combination of user id, password, and complex device identification that creates a digital "fingerprint" of your PC. We also have processes in place to monitor account maintenance and activities initiated through the online banking system.



◆ "Reg E" Protections

Federal Regulation "E" provides consumers with protections for unauthorized electronic transfers. You may be able to recover losses, but you must act in a timely manner. Make sure to notify us *immediately* if you believe your access has been stolen or compromised. Review your account activity and periodic statement regularly.

◆ Protect Yourself

Here are five easy ways to protect yourself from the risks of banking online:

- Choose a complex password involving a mixture of upper case letters, lower case letters, symbols, and numbers;
- Change your password periodically;
- Safeguard your username and password;
- Use a firewall, in conjunction with up-to-date antivirus software and antispyware;
- Log off when you are done conducting online transactions.

For additional tips visit www.ftc.gov or www.fdic.gov.

◆ Internal Assessments

For businesses in particular, we recommend conducting periodic reviews related to the risks posed by keeping old passwords, password retention practices, termination of access rights for former employees, and the adequacy of dual controls. As the risk increases, so too should your protections.

Consider the following: using password encrypted software to house passwords, conducting employee background checks, and segregating duties among two or more people so that no one person has too much access or control.



◆ If You Have Suspicions

If you notice suspicious activity contact Harvest Bank immediately. We will direct you on the steps to insure your account is safe and secure.

We will never email, call, or otherwise ask you for your username, password, or other electronic banking credentials. If you ever suspect that you are being targeted by emails or phone calls, contact us immediately.



Kimball Office
Main Office
75 North Main Street
P.O. Box 70
Kimball MN 55353
320-398-3500

Saint Augusta Office
Branch Office
24952 County Road 7
St. Augusta MN 56301
320-251-6100

Atwater Office
Branch Office
222 Atlantic Avenue W.
PO Box 755
Atwater MN 56209
320-974-8861

Kandiyohi Office
Branch Office
321 Pacific Avenue
PO Box 338
Kandiyohi MN 56251
320-382-6100

Member
FDIC