Recent Scams on the Rise!

In This Issue:

- How to Protect Yourself and Prevent Mail Theft and Fraud
- Don't Dial Trouble: How to Outsmart Phone Phishing Scams
- Stay Safe Online: How to Spot and Avoid Email Phishing Schemes
- Safeguard Your Devices: How to Shield Against Computer Hacking Scams

Mail Theft and Fraud: Check fraud occurs when unauthorized individuals manipulate or forge checks to unlawfully obtain funds from another person's account. Stolen mail presents a significant risk for check fraud as criminals may intercept checks, alter them, or create counterfeit checks to access victims' finances. To prevent mail check fraud, individuals should promptly retrieve incoming mail to minimize the risk of theft. Additionally, employing secure mailing options such as registered or certified mail can add an extra layer of protection against unauthorized access to sensitive financial documents. To eliminate the risk of stolen mail, directly deliver any outgoing mail to your nearest postal facility.

Individuals should promptly report any suspected instances of stolen mail/unauthorized check activity to Harvest Bank and take measures to secure their mail delivery. Check fraud is more common with businesses than with individuals, but anyone can be a victim!

Phone Phishing: Phone phishing is a deceptive practice where fraudsters impersonate legitimate entities to extract sensitive information or money from unsuspecting individuals over the phone. To prevent falling victim to phone phishing scams, it's crucial to exercise caution and skepticism when receiving unexpected calls, especially calls that request personal or financial information. Refrain from providing sensitive details such as passwords, social security numbers, or banking information over the phone unless you initiated the call and can verify the identity of the caller through official channels, such as a legitimate website. Additionally, consider registering your phone number on the national Do Not Call Registry and utilize call-blocking features provided by your phone service provider to minimize the frequency of unsolicited calls. Stay informed about common phone phishing tactics and report any suspicious calls to relevant authorities or consumer protection agencies.

Email Phishing: Email phishing is a fraudulent practice where cybercriminals send deceptive emails pretending to be from reputable sources, aiming to trick recipients into revealing sensitive information or clicking on malicious links. To prevent falling victim to email phishing scams, it's essential to scrutinize emails carefully, especially those requesting personal or financial information. Be cautious of unexpected emails from unfamiliar senders or those containing urgent requests for action. Avoid clicking on suspicious links or downloading attachments from unknown sources. Additionally, enable spam filters on your email account and regularly update your antivirus software to detect and prevent phishing attempts. Educate yourself about phishing and be very cautious about any unsolicited or strange emails.

Computer Hacking Scams: Scammers can impersonate software companies, such as Microsoft or Geek Squad, through various means, such as phone calls, emails, or pop-up messages, claiming there are issues with your computer or software that require immediate attention. They may request remote access to your system or ask you to download malicious software, enabling them to steal sensitive information or install malware. To prevent falling victim to these scams, it's crucial to remember that Microsoft, or other tech companies, do not proactively reach out to users in this manner. Be wary of unsolicited communication claiming to be from a tech company and never provide personal or financial information or grant remote access to your computer to unknown individuals or entities. Install reputable antivirus software, keep your operating system and applications updated, and educate yourself and your family about common phishing tactics to stay vigilant against such scams. If you're unsure about the legitimacy of a communication, contact the company directly through official channels to verify its authenticity.

Remember…

Educating yourself on how to prevent fraud is essential for safeguarding against various scams and schemes. Start by staying informed about common fraud tactics through reputable sources such as government agencies, consumer protection organizations, or financial institutions. Additionally, regularly review your financial statements, credit reports, and online accounts for any suspicious activity, and familiarize yourself with the warning signs of potential fraud. By remaining vigilant, staying informed, and practicing caution in your financial transactions, you can significantly reduce the risk of falling victim to fraud.

If you feel you have fallen victim to a scam and have given out any sensitive financial information, contact Harvest Bank immediately. We are here to help you!

HARVEST BANK

KIMBALL	320-398-3500
ST. AUGUSTA	320-251-6100
ATWATER	320-974-8861
KANDIYOHI	320-382-6100

WWW.HARVESTBANKMN.COM