BORDER STATE BANK *Security Newsletter*

ISSUE: JULY 2018

Welcome...

We handle a vast amount of sensitive information each day. Protecting this information is fundamental to our business. As a result, we have put into place a number of security measures that allow our customers to conduct business securely and with confidence. Technology alone, however, is not enough to thwart the attempts of mal-intended individuals. Security is as much a human issue as it is a technology issue.

While we can provide protections to prevent our Business Online Banking service from being compromised, the customer must be responsible for protecting the security of their own information and PC. We hope this newsletter helps equip you with the security savvy necessary to protect yourself from the various types of fraud. If you find it helpful, feel free to pass it along to your friends, family, and co-workers.

UPCOMING SUMMER EVENTS

07/17/18	***Roseau* Parade**
07/18/18	***Thief River Falls* Parade**
07/19/18	***Thief River Falls* RB Floats**
08/09/18	***Roseau* Comm. Picnic**
08/10/18	***Int'l Falls* Comm. Picnic**
08/16/18	***Baudette* Comm. Picnic**
08/16/18	***Greenbush* Comm. Picnic**

BORDER State Bank
COMMUNITY BANKING AT ITS **BEST!**

CREATING STRONG PASSWORDS

We've taken strong measures to ensure the security and safety of our online banking system, but securing access to your accounts requires teamwork. You can help to keep your assets and computer systems secure by creating and maintaining strong passwords. Using strong passwords that are difficult or impossible to be discovered, and keeping them private, can keep strangers out of your accounts!

Weak passwords are cracked within minutes giving cyber criminals access to online accounts. The more complex the password, the harder it is to crack. It's imperative you take ownership for creating and using strong passwords that act as a barrier between your private information and the thieves lurking about the Internet.

A strong password should:

- Be at least 8 characters in length
- Contain both upper and lowercase alphabetic characters, e.g. A-Z, a-z
- Have at least one numerical character, e.g. 0-9
- Have at least one special character, e.g. ~ ! @ # $ % ^ & * ( ) - _ + =

Examples of strong passwords:

- *Superman is super strong* modified to: **Supermanis$uperStr0ng!**
- *Collect $200 when passing go* modified to: **C$200wpG**
- *She loves you yeah, yeah, yeah!* modified to: **sLuY3ah!**

By using strong passwords and keeping your computer free from malware, you can help us keep your online banking account safe.

PHISHING: *Don't Get Hooked*

"During our regular verification of accounts, we couldn't verify your information. Please click here to update and verify your information."

Have you received an email with a similar message? It's a scam called "phishing"

— A phishing email can look just like it comes from a financial institution, e-commerce site, government agency or any other service or business. It involves hackers and cyber-criminals who are looking to lure personal information from unsuspecting victims. It often urges users to act quickly, to collect personal & financial information or infect your machine with malware and viruses.

How Do You Avoid Being a Victim?

- **Don't email personal or financial information**. Email is NOT a secure method of transmitting personal information. Before sending sensitive information over the Internet, check the security of the website. (Look for https://)
- **Pay attention to the website's URL**. Malicious websites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain.
- **If you are unsure whether an email request is legitimate, try to verify it by contacting the company directly**. Contact the company using information provided on an account statement, not information provided in an email.
- **Keep a clean machine**. Install and maintain anti-virus software, firewalls, and email filters to reduce spam.

What to Do if You Think You are a Victim?

- Forward spam that is phishing for information to spam@uce.gov. Also alert the company being impersonated in the phishing email so they can be alert.
- Review credit card and bank account statements as soon as you receive them to check for unauthorized charges.
- File a report with the FBI's Internet Crime Complaint Center. (*http://www.ic3.gov*)

Spam, phishing and other scams aren't limited to just email. They're also prevalent on social networking sites. The same rules apply on social networks: When in doubt, throw it out. This rule applies to links in online ads, status updates, tweets and other posts.

Is Your Business Protected?

We take our responsibility to our business customers very seriously, and while technology has provided a great convenience, it has also provided many risks. So, how do you protect your business from information compromise?

Here are a few tips to secure your online transactions:

- Offer ongoing training
- Use Multi-Factor Authentication
- Install Anti-virus programs
- Utilize intrusion detection and prevention systems
- Keep operating system current
- Be vigilant with downloads
- Lock your computer whenever not in use
- Schedule an annual third party penetration test

Completing transactions online is not the only way information can be compromised. Make sure your employees understand that they need to secure their computer workstations as well. Passwords should be long and strong and kept private. Ensure that employees do not keep passwords or security tokens in a place that could be accessed by people other than themselves.

By following these simple guidelines, you can protect your customers and your business from everyday cyber-threats.

TOP CYBER SECURITY THREATS

It's a dangerous world out there in cyberspace. Security threats are escalating every year and have become more malicious with cybercriminals stealing financial and personal information. Here's a quick look at some of today's top computer security threats:

1. **Malware.** Exploits and malware are increasing through vectors ranging from social networks to mobile devices to employees themselves. As computer and operating system security continues to improve so will cybercriminals' new techniques to bypass these defenses.
2. **Mobile Threats.** Attackers are turning their attention to launching mobile banking attacks. Keep in mind that if your smartphone becomes infected, it can infect your computer and your home or work network too.
3. **Threats to Mobile Payments.** Electronic currency has made sending money extremely easy. Buying or selling, and sending money from a mobile device is becoming more popular. Hackers know this and are increasingly targeting mobile devices to steal money.
4. **Attacks on SMBs.** Small businesses believe they are immune to cyber-attacks. Truth is, small companies are typically less equipped to defend against an attack and hackers take advantage of that.
5. **User Errors.** Computers are great. For many transactions, they are often better and more reliable than people. Humans make mistakes when using computers, especially when they're not savvy about computer security. Even if you think you're doing all you can to avoid common security threats, you'd probably be surprised at how easily an outsider can find, and take advantage of common mistakes.

Online Shopping DO'S & DON'TS

- **DO your homework.** Before entering your credit card information, take time to research the website and its policies.
- **DON'T buy from spammers.** If you get an email inviting you to buy something like "Discounted Rolex's" you should think two things: 1) spam and 2) possible scam.
- **DON'T forget to inspect your new purchase as soon as it arrives.** If you find a problem, it's easier to fix right away. Notify the seller as soon as possible.
- **DO buy from a website that has encryption.** This feature automatically codes your personal data when it's entered. The URL should start with "HTTPS", "HTTP" is not secure. Also locate the "Padlock" icon to verify a secure connection. Click on the "Padlock" icon to view more information about the site's security.
- **DON'T buy from a web site with which you aren't totally comfortable.** Just remember: "If it looks too good to be true, it probably is."
- **DO use computer security software.** Keep your software updated by applying the latest service packs and patches. Refer to your operating system's help for assistance. This will reduce the risk of contracting a virus or some other form of malware.
- **DO check your credit card statements.** Check your statements regularly so you know when something's awry.
- **DO consider contacting the seller if this is your first purchase.** Most reputable e-sellers have a toll-free customer service phone number. This will assure you that a live person is available if needed after the sale.

ONLINE PRIVACY:
What are you sharing?

Every day, you give away personal information about yourself, sometimes without even realizing it. You do this when you take advantage of all kinds of services, including Internet searches, social networking, mobile and more. What private information are you sharing that you shouldn't? Use these tips to protect yourself:

1. Never give out your full name, address, birth date, or any other personally identifiable information that could be used to impersonate you or gain access to your accounts.
2. Read the privacy policies posted on websites and mobile apps before using their website, purchasing their product, or downloading their mobile app.
3. Update the privacy and security settings on your social networking sites to control who sees your posts and adjust them to your personal comfort level. Don't rely on the default settings. Be aware that both well-meaning and questionable people use social networks to gather information about you.
4. Don't post anything online that you wouldn't mind seeing on the front page of a newspaper.
5. Make sure that your password is long and complex. Don't reuse passwords on multiple accounts. Instead, choose unique passwords for each account, especially your online banking account.
6. Log out of websites and browsers when you're finished using them. Never leave your online accounts open.
7. Be wary of sites that offer a reward or prize for clicking, filling out surverys, or providing other information.

Our Locations

BADGER
202 Main Street
Badger, MN 56714
218.528-3255

BAUDETTE
605 Main Street
Baudette, MN 56623
218.634.3300

COON RAPIDS
9950 Foley Boulevard NW
Coon Rapids, MN 55433
763.780.6600

GREENBUSH
133 Main Street
Greenbush, MN 56726
218.782.2151

INTERNATIONAL FALLS
1414 Highway 71
Int'l Falls, MN 56649
218.283.5556

LANCASTER
114 Central Ave S
Lancaster, MN 56735
218.762.6222

MIDDLE RIVER
150 Hill Avenue
Middle River, MN 56737
218.222.3511

ROSEAU
1083 Third Street NW
Roseau, MN 56751
218.463.3888

THIEF RIVER FALLS
1528 Highway 59 South
Thief River Falls, MN 56701
218.681.8085

BADGER | BAUDETTE | COON RAPIDS | GREENBUSH | INTERNATIONAL FALLS
LANCASTER | MIDDLE RIVER | ROSEAU | THIEF RIVER FALLS

www.borderstatebank.com | **24HR Voice:** 1.866.BSB.24HR | Member FDIC

BORDER State Bank
COMMUNITY BANKING AT ITS **BEST!**