FALLS CITY NATIONAL BANK

Cybersecurity Tips

Establish strong passwords.

- Where available, take advantage of multi-factor authentication.
- Make your passwords at least 8 characters, preferably 12.
- Always use upper- and lower-case letters, numbers, and special characters.
- Do not write your passwords down, particularly next to your computer.
- Do not use personal information such as birthdays or last names or the city where you were born.
- Don’t use common words such as “password, welcome” etc.
- Never use sequential numbers such as 1,2,3,4,5.
- Never share your passwords.
- Have different passwords for different places. (i.e. have different passwords for each device.)
- Change your passwords often.
- Change your security questions often.

Secure your mobile devices.

- Keep all applications and operating systems current.
- Delete any applications that you don’t use.
- Do not use public Wi-Fi.
- Use strong passwords.
- Do not store sensitive work information on your personal device.
- Don’t download applications from third party app stores.
- If you are connected to your company’s system (i.e. network, email), make sure you have the company’s encryption method on your device.

Never leave your devices unattended.

When you leave your computer, always lock it so no one can use it while you are gone.

FALLS CITY NATIONAL BANK

Cybersecurity Tips

Stay cyber-safe on the web.

- If a website requests your Social Security Number or your username and password for other services, then it most likely is a scam.
- Check for a phone number, email address, or other contact information on the website. If they provide it and it is in service, this will give a good indication that the website is legitimate.
- Check the site to see if there are any obvious misspelled words or other indications that it is a fraud.
- If you put your mouse pointer over a link it will reveal its true destination in the bottom left hand corner of your browser. If it is different than what the link says, then discontinue use of the site.
- Don’t enter any personal information on a site that doesn’t have a padlock in the browser window and an https:// at the beginning of the web address. It’s most likely not a secure site.
- Once you get to a website, check the address in your browser’s address bar to make sure it matches the address you typed. The bad guys are good at making fake sites look real.
- Make sure to log out of any secure site before closing your browser. Just closing your browser will not automatically take you off the site.
- Make sure your anti-virus software is up to date, and all updates have been applied.

Secure your mobile phones.

Smartphones hold a lot of data. You should consider them just as valuable as a company computer. They’re very easily lost or stolen, and as such, securing them is high priority. These devices should be encrypted, be password protected, and have “remote wiping” enabled.

FALLS CITY NATIONAL BANK

Cybersecurity Tips

Update all computer programs regularly.

Properly patching and updating each computer and its programs and applications regularly is very important to overall enterprise security. If systems and programs are not properly maintained, it can quickly become a problem. Your software and applications are only as good as their most recent update.

Install good antivirus protection.

In terms of your online security arsenal, good anti-virus and anti-malware software are essential. These important programs are your last line of defense should an attacker get through to your network.

Look out for fake check scams.

In some fake check scams, you will be sent a check with instructions to deposit it and wire some of the money back. The check may look legitimate, but if a request is made to wire money back after depositing a check, it most likely is a scam.

Beware family emergency scams.

This is a scam wherein you will receive a call from someone who claims to be a member of your family that needs cash for an emergency. They will ask you to wire money right away and to keep the request confidential. Before you send money, talk with your family to verify the caller.

Monitor your accounts for suspicious activity.