CyberSecurity Quarterly

Stay Protected

Hackers many times rely on "holes" found in a given device's software. These holes are fixed with software updates. All PCs, phones, tablets, etc. come with periodic updates so it is best to run them as soon as you are notified. Another great way to assist with any potential malicious software being installed on your system is to have an antivirus program installed on the device.

Stay Skeptical

Did you just receive an email stating you won a large sum of money? Does your inbox contain an email from your internet provider stating you need to email them your login information immediately?

Chances are if it is too good to be true then it most likely is. In addition, if your gut is telling you something is off about a given situation in the technology realm then most times it is wise to listen to it.

If you are still deciding a given email or popup is legitimate it is best to call and talk to an actual person to verify.

What is CyberSecurity?

CyberSecurity is defined as the state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this. Data, in this context, is basically any information pertaining to you as an individual. All of your financial, social security, and other confidential information is electronically stored somewhere. With this in mind it is important to know what you, as a customer, can do to protect yourself.

The physical location that stores this information has, or should have, the latest security hardware, software, and other security measures in place to make it as secure as possible. No network is 100% secure which tells us there is always a degree of risk. The ultimate goal of CyberSecurity is to use best practices to minimize the risk.

Dakota Western Bank follows CyberSecurity best practices by having a security strategy and policies that will always provide you with the absolute minimal level of risk of your information.

dakota western bank Member FDIC EQUAL HOUSING LENDER

What if I clicked on an email I shouldn't have?

If you suspect you are infected, shut down your PC immediately (by holding down the power button if needed) and take it to your local technology repair center. They will be able to run tools on the device to determine if your device has been compromised. If your device has been compromised it is always best to restore the device back to factory default and change your account passwords in case that information was stolen.

What if my password has been stolen?

One common situation which can be a result of a stolen password is simply getting a legitimate notification stating someone has logged into your email from a location which you haven't logged in from before. Another common scenario is the attacker using your email account to send out email on your behalf (sometimes to spread malicious email to your contacts). In this case you may receive replies from your contacts to emails you don't recall sending. The two common scenarios above suggest your login information has been obtained from an unauthorized party. It is recommended you change that password immediately. If your inbox contained any other login information for other accounts, it is best to change those passwords as well.

Threat of the Month

Tech Support Scam

You are browsing a website you normally visit and receive a pop up similar to the one below stating you are infected. The pop up says to contact the listed number immediately. A common number listed claims to be Microsoft. Microsoft will NEVER contact you directly. Upon calling the number they will ask to remote into your PC and look like they are "fixing" your PC. In reality they are installing programs in the background designed to steal your information and have access to your device at will.

Security Tidbits

What is multifactor authentication (MFA)?

Multifactor authentication is a method of confirming a user's claimed identity only after successfully presenting two or more pieces of factors to something a user knows (password or PIN), possesses (phone or card), and/or is (fingerprint).

A common example of this in the real world are sites using a password and a code generated on your phone to successfully login. Since a potential attacker will not have your phone this provides an additional layer of security. It is always recommended to enable this feature if available.

dakota western bank Member FDIC EQUAL HOUSING LENDER