Decorah Bank & TRUST CO. Cresco Bank A DIVISION OF DECORAH BANK & TRUST CO.

1-2-3 Banking

Strong beginnings to a healthy financial future

Fraud Prevention One-Oh-1

Take a minute to think about all the ways you are connected to the world. Do you have a smartphone? Some kind of tablet? What about a smart TV? Perhaps you own a gaming system with online capabilities. The average U.S. household actually has 5.7 connected devices, and that number is going to rise. In the mind of a savvy hacker, that means 5.7 ways per home to hack in and steal valuable information. With some simple steps, you can stay secure.

Powerful pA$$w0Rds.

Creating a strong password is the easiest way you can protect your valuable information (like bank accounts). Put passwords on as many things as you can, like your home Wi-Fi, smartphone, or laptop. Try to create a password that has eight or more characters and mixes numbers and symbols in place of letters. Do not ever share your password with anyone! Legitimate companies will never ask for an account password. If you get a phone call from some service claiming to help you achieve something, and they ask for any kind of website password, beware! This is a common practice for fraudsters. Fun fact: The top two most commonly used passwords in the U.S. are “password” and “123456”. Don’t be one of those people.

Biometric Security.

While it isn’t everywhere yet, you can find biometric security now on many smartphones and laptops. If you have a device that offers this, use it. Unless a fraudster has your fingerprint or an exact copy of your retina, they will be unable to access anything you want to protect. Be on the lookout for this kind of technology to emerge more in the future.

TBYC (Think Before You Click).

This acronym is not an ice cream store, but an easy to remember phrase to help you avoid the unwanted hassle of being hacked. The dangers are all around – pop up ads on your smartphone, malicious websites on your laptop and fake apps on your tablets marketplace (fraudsters created a fake Angry Birds app, designed to install a virus on smartphones). When browsing the web, look at the websites URL before you click. Does it seem legitimate? Does it end in something common like .com, .net, or .org? In the marketplace, look at the reviews and comments before you download an app. Many clues to the legitimacy of an app can be found there.

From bank accounts to social media websites, you have valuable information everywhere. By following some easy steps, you can save yourself from a big headache. Check out https://www.dhs.gov/topic/cybersecurity for more detailed information on cybersecurity. For information on what the bank does to protect your information, give us a call. Enjoy the journey!