Digital Deception: Watch Out for Cybercrime - Video Transcript

As online commerce and recordkeeping have expanded, so has cybercrime.

Private companies and government agencies that hold personal information are responsible for protecting that data, but even the most vigilant organizations can be vulnerable.

Cyber thieves have a number of tricks up their sleeve to unlock your data, and once a data breach occurs, the aftershocks can last for years as thieves exploit stolen information.

Thieves can guess online passwords and/or security questions and trick you into providing information through bogus “phishing” emails.

So how can you protect your data online?

The first line of defense is a strong password, which should be eight or more characters long and include a combination of lower-case letters, upper-case letters, numbers, and symbols.

Avoid using easy-to-guess passwords like 1-2-3-4-5-6, sequential letters on a keyboard, or even the word “password.”

Use a two-step authentication when available, which requires a text or email code along with your password before you can access an account.

Restrict the use of your Social Security number to secure government sites.

Before providing any financial information, look in the address bar for the secure lock symbol and the letters “https:” as opposed to just “http:”

And never click on unfamiliar links in emails and texts.

Outside of cyber world, protect your health insurance ID card as you would a credit card to combat the growing risk of medical cybercrime and be aware of anything that looks amiss at card payment terminals, especially in remote locations.

And what about mobile payments?

Paying with your smartphone could be safer than paying with plastic as long as you take the same security precautions you would on your computer and you use security enhancements such as fingerprint access.

Even with careful precautions, it’s important to monitor your accounts regularly to stay vigilant against cybercrime.