Summer has faded into memory as the cool mornings and frosty windshields confirm winter is coming. As the calendar slides through the “ber” months, the holiday season arrives on the heels of the colder temps and snowy landscapes. Soon, friends and family will gather to watch football, heap plates full of food, and have dynamic conversations about the politics of both the family and the nation. In preparation for these upcoming festivities, the holiday shopping season takes center stages for many.

Shopping transactions in our modern world are almost exclusively done with digital payments. Paying with a credit/debit card or one of the many payment apps on our devices is easy, convenient, and preferred by most retailers. As the use of digital payments has increased, so too has the effort criminals have put into illicitly obtaining private identifying information (like social security numbers) or digital payment information (like credit card numbers). Every day, thousands upon thousands of campaigns aimed at breaking into financial systems are initiated by cyber criminals across the globe. These criminals run a numbers game, probing for weaknesses in security systems over and over until they find the weak link in a security system somewhere and exploit this weakness to break in and steal what information they can find.

We hear about these security breaches regularly in the news and I’d venture a guess that many of you reading this have received at least one notice in the mail because your data was stolen from a database somewhere in the world. While there is little that the average person can do to stop these security breaches, each of us can take a few small steps to avoid being a victim.

Scrutinize online retailers when shopping. When using a browser, at a minimum, you must ensure your connection is secure. The web address should start with “https:” to signify a secure connection. The browser’s address bar will also have some kind of symbol to tell you if the site has valid credentials. Depending upon which browser you use, this might appear as a padlock, a dropdown button, or another symbol that when clicked or hovered over will tell you if the site has valid credentials. If shopping through an app, ensure that you have downloaded the app from a trusted source (like Google Play or the Apple App Store).

Pay attention to payment portals when shopping in person or using an ATM. Criminals have developed skimming devices that capture and store credit card data. Skimming devices are most commonly placed in locations not regularly staffed by an employee, like a gas pump or an ATM. These devices are made to look like a legitimate card reader. Take a close look at card readers for any sign that a skimming device has been placed on top of the legitimate card reader. Look for misalignment of panels, missing or broken security seals, or a mismatch of the texture or color of the card reader from the surrounding machine.

Stay on top of your credit report and banking transactions. Even the most diligent employment of crime prevention measures with digital payments still leaves the person vulnerable to the weakest link of the retailer’s security measures. With financial information breaches happening regularly, the best defense against becoming a victim lies in being vigilant about your credit report and banking transactions. Everyone is entitled to get one free credit report from each of the three major credit bureaus (Equifax, Experian, and TransUnion) annually. In addition to the free annual credit report required by law, each of these three credit bureaus allow consumers the ability to obtain a free credit report once per week. Free credit reports may be obtained at AnnualCreditReport.com and more information about credit reports may be found on the website of the Federal Trade Commission. A credit

report will show you all the accounts open in your name. It is important to review these regularly to ensure you've not become the victim of identity theft due to a data breach.

For those who don't wish to go through the steps of routinely obtaining a credit report, subscribing to a credit monitoring service is a great prevention step. Credit monitoring is available from several providers. For a regular fee, these providers will monitor your credit reports and provide updates if anything changes. This monitoring can provide early warning that someone is attempting to open an account in your name without your permission.

An even simpler solution is to place a freeze on your credit report. Freezing your credit requires a person to contact all three major credit bureaus and request a freeze. While the freeze is in place, no new accounts may be opened in your name, by you or anyone else.

Finally, make use of online banking features that detect fraud or provide notice of any transactions posted to your accounts. Most financial institutions have programs to detect and prevent fraud and are happy to work with their customers to ensure the customer has the level of notification and detection they are comfortable with. These tools allow people the ability to stop unauthorized transaction before they are completed.

Master one or two of these crime prevention strategies for digital payments to help avoid being the victim of a grinch and, as a bonus, you'll have a great new topic of conversation for your family gathering when you desperately wish to shift the topic of conversation. For more crime prevention information and safety information visit the Benton County Sheriff's Office website at: https://www.co.benton.mn.us/211/Crime-Prevention. You can also like and follow us on Facebook and Twitter at @BentonMNSheriff for regular updates and crime prevention messages.