

Let's Talk Finances

Money Safety Tips



By Charles Schmalz
President of
East Wisconsin Savings Bank

By the end of the year, an estimated 1.92 billion people will be digital buyers. That means around 25% of everyone on the planet shops online. With that many consumers on the web, it's no surprise that criminals are flocking to the digital space, too. You can fight back against the hackers and frauds who may try to steal from you with a few precautions and common sense. Protect your wallet when shopping online by paying attention to the tips below:

Monitor Your Accounts

Proactively monitoring your financial accounts (such as bank and credit card statements) can help you catch errors and spot potential fraud at the first sign. To simplify this process, consider using a single credit card for all your online purchases. That way you will only have one statement to check instead of several. This practice has the added benefit of reminding you to stay on track with your budget, too.

Always Think Before You Click

To avoid infecting your computer or mobile device with malicious software, never click on a link to a deal or special savings on a social networking site or in an unsolicited email. Scammers will often disguise a social media post or email to make it seem as if it's coming from a known retailer, but the link will take you to a fake site and infect your device. If you see a link that supposedly leads to a sale you want to take advantage of, visit the retailer's website directly rather than clicking the link. From there you can verify if the sale is legitimate.

Avoid Public Wi-Fi

Online purchases require transmitting your credit card, bank account information, or other financial information over the internet. Using a public Wi-Fi connection to do so puts that sensitive information at risk. Hackers can tap into unsecured Wi-Fi connections at hotspots like coffee shops and airport terminals to capture it without you knowing. The new, more secure EMV chip cards do not protect against this kind of fraud. If you're using a wireless connection to shop, be sure that it requires a password or WEP key. Also look for "https:" in the website address (rather than just "http:") to be sure the website itself has security protections in place.

Be Proactive

Finally, take action if you hear about a data breach or other fraud that could affect your accounts by changing your passwords. This is especially critical if you use the same password on multiple accounts. If you notice suspicious charges on your credit card or transfers from your banking account, contact your bank right away to notify them of the issue. They may put a freeze on the account to prevent further fraud, but this will keep the criminals from emptying your account.