



— HAPPY CYBERSECURITY AWARENESS MONTH! —

October is a time to remember that your security and protection of personal information should remain top priority. Whether you own a small business, work for a large corporation, or simply keep digital records at home, your computer and other digital devices store a lot of information and data. You might think you're safe from fraudsters looking for a way to steal your personal information. Who would want your data anyways, right? However, you might be surprised to know that security breaches on computers have been steadily increasing every year, alongside ransomware attacks.

Additionally, since the start of the COVID-19 Pandemic, the FBI has reported a 300% increase in cyber-attacks. Fraudsters are taking advantage of people having a little more time on their hands, working from home and utilizing online learning tools for kids.

Knowing where to start to protect your information can feel overwhelming, and we want to help you and your family keep personal information safe. Here are some ways you can protect yourself and increase your cybersecurity!

Take Your Password Security Seriously

You've heard it before: be vigilant about your password security! Passwords that are simple, easy to crack, and used for multiple accounts are an easy target for fraudsters. Passwords have become a part of our everyday lives; our phones, online accounts, and computers are protected by passwords to keep information safe. Despite an emphasis placed on strong passwords, many people do not follow safe password standards, creating a chasm in cybersecurity. Hackers are finding it relatively easy to crack passwords, because as soon as one password is exposed, all your other accounts with that same password are also at risk.

Some things to consider when creating and managing your passwords include:

- Avoid common words and phrases
- Don't use personal information
- Never recycle passwords
- Utilize a password manager or generator

We know just how frustrating and confusing it can be to manage all your passwords, but making password security a priority will help ensure that your accounts, such as your bank account and streaming services, are safe.

Don't Over Share on Social Media

With folks having limited interactions with friends and family, many have turned to social media as a source of entertainment and to connect with those they love.

However, there are also risks that come with sharing too much information on these platforms.

One specific risk is sharing too much personal information via surveys, quizzes, and questionnaires on social platforms. Users will typically fill out or answer these quizzes, and then share with friends and family that they are connected to. While seemingly harmless, your answers could be used by fraudsters to access accounts.

Because many online platforms will utilize security questions to authenticate a user, the quizzes or questionnaires on social media will often ask the same or similar questions. Fraudsters use the information garnered in the quizzes and questionnaires to answer these security questions and gain access to your account, leaving your information in a vulnerable place.

The best thing you can do is limit your answers on these quizzes and don't over share! By filling out these quizzes, you may unknowingly give away answers to questions that are used to unlock or authenticate access to an online account.

Install Updates ASAP

While this task is tedious, installing updates on your digital devices is a surefire way to combat cybercriminals. Outdated and unsupported software can pose a serious security threat, as it can be exploited by cybercriminals to gain access to information on your computer. Updates are designed to close off avenues of access from unwanted third parties and keep your information safe. Installing updates as soon as they come out is the best way to lessen the likelihood of encountering an issue due to outdated software. Set your computer to update automatically, use automatic updates on your browser, and be sure to keep extensions, such as flash and java, fully up to date.

Avoid Public Wi-Fi

This is especially important for kids who are utilizing online learning for the school year. As many kids started the school year at home, it is so important to make sure you are accessing safe and secure Wi-Fi. Public Wi-Fi hotspots, while convenient, are where cybercriminals can gain access to important information. Many of these networks are un-secure, and those with the know-how can view your information while connected to that Wi-Fi hotspot. If you must use public Wi-Fi, always use either a VPN or, if that's not possible, use the data on your mobile device to access the information you need.

Here at Blackhawk Bank, we want to make sure your computers and phones are safe, so your information doesn't end up in the hands of cybercriminals. In honor of Cybersecurity Awareness Month, take some time to make sure your information is safe and prioritize cybersecurity with your family! To learn more about information security, check out the National Cybersecurity Alliance at www.staysafeonline.org. If you are interested in learning more about how Blackhawk Bank can help you, [contact us today!](#)