October is Cybersecurity Month: 7 Steps to Stay Safe from Threats

The number of consumers and companies affected by cybercrimes continues to increase every year. It is estimated that cybersecurity incidents increased by 38 percent from 2014 to 2015, and the average cost per person incurred per stolen record was $154. As a result of 781 publicly acknowledged data breaches over 169 million personal records were exposed.

The threat to your personal information continues to grow. October is Cybersecurity Awareness Month and is the perfect time to learn how to better protect yourself. The number one protection against cybercrime is an informed consumer.

#1: Use More Than One Password
Many people use the same password for multiple accounts, which means that if your credentials are stolen for one account all your accounts are in jeopardy. Do you really want to give criminals access to your bank account because you used the same credentials for your free online music account?

#2: Use Stronger Passwords
No matter how secure a financial institution or shopping website may be, if your password is easy to guess you are still at risk of fraud. Do not use your name, birthday or pet's name, as this information is readily available to many people, especially if you post it on social media. The best passwords are often derived from an entire phrase, rather than a single word, and incorporate letters, numbers and special characters. For example, the song lyric "Don't worry; be happy" can be transformed into this password: d0ntwry_Bhpy.

#3: Beware of phishing scams
The dangerous thing about phishing scams is they don't rely on weak website or network security. Instead, they attempt to crack the human firewall: you. Phishing scams attempt to obtain personal information or plant a virus or malware on your device by sending a fake email requesting that information, or instructing the recipient to click a link in order to reset their account.

Never give out your personal information over the Internet, phone, or via text message unless you know exactly who you are dealing with. If you receive a suspicious email from a business or charity and you're not sure if it's legitimate, close the email, open a new browser, visit their official website and contact them through their customer service. There is often an increase in phishing scam attempts after heavily publicized security breaches (pretending to offer account security) or natural disasters (fake charities), so be especially on guard in those situations.

#4: Avoid using public Wi-Fi to Buy
If you frequently shop online, keep in mind that any purchases made via the web require transmitting your credit card and/or bank account 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 that information. If you're using a wireless connection to shop, be sure that it requires a password or WEP key. Websites that have additional security protections have https:// instead of http:// on all pages of the site.

#5: Monitor Your Credit Report
Your credit score affects many aspects of your life, including interest rates on large purchases, obtaining loans, and even renting an apartment. Make sure you check your credit report three times per year (one for each of the three major credit reporting agencies: Experian, TransUnion and Equifax). You can do so for free by visiting www.annualcreditreport.com. Watch for unauthorized accounts, loans or purchases because they will damage your credit and signal that your identity may have been stolen. If you find inaccuracies in your report, you can dispute those errors online, by mail or over the phone by contacting the credit bureau where you found the inaccurate report (contact information will be on the report itself).

#6: Be careful what you throw away
Dumpster diving doesn't just apply to paper statements and discarded credit cards anymore. Before you recycle or donate old cellphones or computers, be sure to remove any personal and financial information. For computers, the best way to do this is to use a wipe utility program to overwrite the entire hard drive. For mobile devices, check the owner's manual, service provider website, or device manufacturer's website for information on how to permanently delete information. In addition, remove the SIM card from the device.

#7: Take Action
If you hear about a data breach or other fraud that might possibly affect your account, be proactive and change any related passwords. This is especially critical if you use the same password on multiple accounts (which you should avoid doing anyway). 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.

BankFirst
NATIONAL
For Better Banking, Think First.

More Consumer Column articles are available at www.BankFirstNational.com under the About tab.

Article courtesy of the Wisconsin Bankers Association / Consumer Column