BY MEGAN BURMESTER AND MORGAN STASHICK

CYBER-CRIME, NOT ON YOUR DIME

How many passwords do you juggle and try to remember daily . . . five? Ten? Since it can be difficult to recall so many, we may not be as shrewd as we should be when creating and updating passwords to keep track of our accounts.

In this day and age, we're surrounded by Internet connectivity, smart phone apps, email, and all kinds of social media. The average computer user maintains multiple usernames and passwords ranging from Facebook to email to accessing online bank accounts. Unfortunately, the more accounts we have, the higher the risk of hacking, particularly if we don't manage our passwords. Prevention is the best way to not become the next victim of cyber hacking. Anthony Skjellum, director of Auburn's Cyber Research Center, provides tips on how to help keep your personal information from getting into the wrong hands.

Keep passwords long. Skjellum says keeping passwords long – 24 characters or more— makes it more difficult for them to be hacked. For instance, select a lengthy, memorable word or phrase, followed by your favorite number for added security. It is recommended to change your password every three months – even if you keep the word the same, simply change the number at the end systematically so it is easy for you to remember. Don't share your passwords, update them periodically, and never reuse old ones.

Choose security questions and answers wisely. When creating online accounts, users are often required to choose a security question to be asked if they forget their password. Many sites and apps offer standard questions to choose from including, "What's your mother's maiden name?" and "What's your pet's name?" These common responses make it much easier for a hacker to guess and end up costing you in the long run.

If possible, it's best to use the option of writing in your own, unique question and answer. The answer to your security question should be something that is not easily guessed, recognized, or researched, so a hacker cannot answer the question and gain access to your password. Add a number to the end of the question for added security, or even better, make up a false answer to ensure nobody can guess it.

Lock your phone. If anyone were to get their hands on your phone, make it harder for them to access your information by having a lock code in place. Skjellum suggests turning on your phone's "Remote Disable" setting, which will erase personal information from your phone on the chance it is stolen. Likewise, having the "Find My Phone" setting activated allows you to see the GPS location of your phone if it's ever lost or stolen.

Use credit cards and cash, not debit cards. Credit card companies are liable for charges that show up on your statement that you did not purchase if your card is stolen. That may not be true of debit cards – losses may end up being your responsibility, up to the whole balance of your account.

Use common sense. Don't open unfamiliar email attachments, or suspicious email (have you seen the subject lines stating, "If you wire me $100 for my ailing great grandma, I will return the favor with $100,000?" Don't fall for it.) These are most likely computer malware.

Remember to shred all of your paper documents, because it's common for people to dig through trash to look for social security numbers and credit card information and enjoy a shopping spree on your dime. Not every crime is a cyber-crime.

Test your passwords strength and find out how long it would take a hacker to access your account by visiting https://howsecureismypassword.net/