Protect Yourself from Hackers

And Cyber Thieves

In Today's fast paced world of technology and plastic payment options, our Phones, Computers, Tablets and Debit or Credit Cards have become the norm for our daily lives. Hackers are getting smarter and smarter and it is very important that we stay protected against the threats they pose. You will read below, a list of ways to protect yourself and your accounts.

Passwords

Passwords are an important part of securing our accounts. It's never a good idea to use the same password for all of your accounts and it is a good idea to change them every few months. Use passwords that are not easy for hackers to figure out. Passwords such as "Password1" "123456" or "qwerty " are bad password choices and will easily allow hackers access to your devices or accounts. Use complex passwords containing at least 8 characters, up to 64 and use a combination of upper case, lower case, numbers and special characters to make your passwords strong. You can also use a phrase as a password. If you have many passwords, write them down and keep them in a safe place, not on your computer.

Anti-Virus

Using Anti-Virus is of the utmost importance. Hackers like planting spyware, key loggers, viruses and malware on unsuspecting computers. If you open an email or click on a file attachment and it doesn't do anything that you can see, it's probably bad and your computer will be at risk of a hacker gaining all of your passwords and possibly all of your account information. Stay away from anti-virus programs claiming to be free. Use proven Anti-Virus/Malware software that remove viruses, malware and spyware in real time. It's also a good idea to protect your hand held devices and Tablets.

Phishing Scams

These scams send bogus emails and could appear to be from family members, utility companies or other entities. These hackers will try and gain as much information as possible on you. If they get enough, they will try to open credit card accounts in your name or if you give them debit or credit card information, they will duplicate your accounts and drain you dry. Utility companies and most businesses will not do collections via email. If you question the legitimacy of an email, simply make a phone call to the provider and ask if they had sent you an email. A phone call will save you a lot of time and possibly money in the future.

Elderly Scams

Elderly Scams target older people claiming a family member is in jail or has been in an accident and needs money. Hackers do research on people before making these calls and they may seem authentic, but usually are bogus. Never give out bank account or personal information to anyone over the phone or via email.

Microsoft Scam

You might get a random phone call from a person from Microsoft or see a pop up on your computer saying your computer has a virus and they need to check it out and can fix it. Never fall for this scam. The person will want to gain remote access to your computer and usually will steal whatever personal information they can get on you and then inject malware or a virus on your computer and then charge you money to remove it. Do not let anyone ever remote into your computer. Scammers also claim to be from other businesses like Readers Digest or other well-known companies. Hang up on these callers and do not play their game.

Pre-paid Money Services

Hackers will try and get you to go to the store and either use Western Union, MoneyGram or Green Dot pre-paid cards as form of payment. Be very suspicious if someone asks you to use one of these payment types. Typically it's a scam.

Gas Pump Scams

These scams have been going on for many years. To protect yourself against gas pump scams, simply use your credit or debit card inside the store and not at the pump. It's not as convenient, but it's safer.

Cybersecurity is not a sprint, it's a marathon.

1: Update your computers, phones and tablets to the latest software versions and check for updates on a regular basis.

2: Update antivirus definitions daily, or each time you use your devices if it is not daily. Regularly scan your computer for malware, spyware and viruses.

3: Change passwords every few months and make them complex. The industry standard is 8 characters containing Upper and lower case letters, numbers and special characters.

4: Never give anyone remote access to your computer or Tablet.

5: Be suspicious if you get a call or email from strangers wanting personal info. If in doubt, follow up with phone calls to ensure the authenticity. Do not call a number the person on the phone or in an email give you, often they are bogus.

Gouverneur Savings & Loan Association