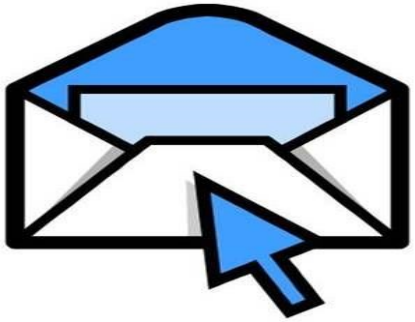

Email Security

While email is a wonderful tool, it can also be a hacker's window into causing you grief and heartache. You can lessen your chances of being scammed by keeping these ideas in mind:

⇒ When emailing people who don't know each other, always use the BCC: option. (Blind Carbon Copy) This way, people receiving the email won't see other people's email addresses.

⇒ Financial organizations will never (let me repeat that, never) email you and ask you to verify your information by clicking on a link. Never, ever give your password or pin or Social Security number through an email.

⇒ Package delivery companies (UPS, FedEx, etc.) will never send you an email with an attachment.

Don't Let Panic Rule

Those trying to access your computing device and/or accounts will stop at nothing to trick you. Your job is to be knowledgeable enough to not fall for what they are selling. Here are some of the ways they try to panic you into making a wrong choice:

They'll create a program or Internet site that warns you: "Your IP address is showing on the Internet and your financial information may be at risk." Scary thought, isn't it? News flash—everyone's IP address shows on the Internet. Do you have a house number on your mailbox or the side of your house? Most of us do. But, driving down the street and seeing that doesn't tell us anything about the person inside or about their finances. Don't be fooled by this fake message.

A hacker will create a website and lure you there through search. Once on that site, you may see the site "scanning" your computer. It will warn you that you have x number of viruses and x pieces of malware and you are at risk. Sometimes, they'll give you a phone # to call. Never call the number – this will always be a scam. If you can't get off the page, force your computer to shut down by holding the ON button 8-10 seconds. If the same message reappears after restarting your computer, call a computer person.

You'll receive an email saying your email account is full and will be turned off if you don't "click here." Don't do it. In 99.9% of the cases, this is a scam email.

Computing Security

A brief review of computing security. Presented by Keystone Computer Concepts, Inc. where

"*We Speak English, Not Geek.*."

Always have a good anti-virus program and keep it up-to-date.

4KCC
KEYSTONE COMPUTER CONCEPTS
WWW.4KCC.COM

Social Media Security

A Hacker's Playground

In the last quarter of 2018, Facebook reported that it has 2.32 billion (yes, that a "b") active, monthly users. That many people in one place attracts hackers!

If you use social media sites, here are some insights:

- Post your vacation pictures after you are back home. Posting while you're away may give the bad guys all the info they need to clean out your home of valuables.
- Keep your profile locked down—every social media site has security settings and you should know how yours are set.
- Remember that, if you are on social media, privacy is no longer an option for you.
- Never type in your password if you're already logged in.
- Don't post pictures of others without their knowledge and permission.

Passwords

According to SplashData, the top two worst passwords for 2018 were "123456" and "password." Are you using easily-hacked passwords? Take a moment to read some of our password rules.

Password Rules

1) Passwords should be created using the FBI's procedure for creating passwords. Take a phrase containing a minimum of 4 words, use the first letter from each word and, in between, place numbers that you can easily remember. Add a symbol to make the password stronger. Example: my phrase: I love Hershey's chocolate. My numbers: 1767. My symbol is an asterisk (*). My password becomes: I1l7H6c7*

2) Don't use the same password for everything!

3) Keep your passwords in a secure place—NOT a text file on your desktop (or anywhere else on your device) —or use a Password Manager.

4) If you change your password and you're not using a Password Manager, write down the date beside your new password and scratch out the old one.

5) Update your account password recovery information before you need it—update your alternate email, your cell phone # and your security questions.

6) If you think your email or other accounts have been hacked, change your password immediately.

7) Don't give your password to anyone you absolutely don't know and trust.

8) Never use any portion of your Social Security number or your user account name as part of your password.

9) If the site provides the opportunity, turn on multi-factor authentication – this can be text messages to your cell phone or, better yet, using an authentication app like those available from Google and Microsoft.

Contact Us

Keystone Computer Concepts
1767 SW Leafy Rd
Port Saint Lucie, FL 34953

(772) 408-4425 * techs@4kcc.com

Visit us: on the web: www.4kcc.com
On Facebook/Instagram: 4Keystone
On Twitter: @4KCC