Human Factor

This information is presented as general purpose suggestions and the effects may differ on each device or based upon specific updates done to each device. The County of York assumes no liability to unintended results this may have on your specific device and will not assist in any issues that may arise from implementing these tips. This is not an all-inclusive list of all software options available, simply a partial list of some options for the reader to further research for what might work best for them.

Modern day IT devices have stronger security than ever before and generally they are shipped with most of the security features enabled. For the last several years hackers have changed their tactics and have begun mostly focusing on the weakest link, people. This takes many forms: from cyber stalking to social engineering. Social Engineering is when a hacker manipulates individuals into divulging confidential information for fraudulent purposes. For most of these people these cons are their full-time job and unfortunately they are very good at it. When someone realizes they have been taken advantage of, they are usually ashamed and are afraid to speak out in fear of what others will think of them. Again, these are victims of professional con-artists and unfortunately part of a growing group of victims. By sharing their experience, they can help other avoid the same pitfall. Below I will share several tips and strategies to avoid being an easy victim.

Online Privacy

Social media is a normal part of most people's lives and is highly integrated into our society. To be safe on the Internet doesn't mean you must abandon these services, simply that you should think before you post.

1. **Avoid Schedules** – One tool for modern day burglars is to check the social media feeds of their soon to be victims. If you post information about how your family will be at Disney World for a week you are also potentially announcing to criminals that your house will be vacant. While hiding this type of information may not be practical, be aware of the increased risk. As a side note, many local Sheriff or Police departments will offer to check on your home while you are away for a prolonged period (assuming the deputies/officers have available time).
2. **Avoid contact information** – When using social media, auction, or selling websites avoid posting your home address or direct phone number. Usually you want to meet the person in a public location (some jurisdictions even offer "safe" locations for this purpose). You also want to communicate with them over that website or application whenever possible. Realize that there are people who stalk these sites pretending to sell cheap used vehicles or in search of personal information they can sell or use themselves. Most of these websites will have lots of tips and warnings, please read and follow them. If the person is demanding to pay via money order, wants a wire fund (e.g. Western Union), or talks about a third party guarantee is probably trying to scam you.

Reference: https://www.craigslist.org/about/scams

Phone calls / Spam

Another very common avenue for many con-artists is to call the target on the phone. Follow the tips below for any unsolicited phone calls asking for information.

1. **Don't share information** – Unfortunately, when someone calls you should initially not believe they are who they say they are, you should always be skeptical. Some examples would be, "Why would my credit card company be calling me asking me for my card number?" or "Why would my bank be calling me and asking me for my home address?" If you think they really could be legitimate, ask for their name and the company and tell them you will look-up their number (such as your bank's main number) and ask to be transferred to that person. I will let them guide me how to get a hold of them but all based off a phone number that I find related to the company, never a phone number they give me (since I have no way of knowing that the phone number is really with that company).
2. **Don't believe caller ID** – Unfortunately, there are many ways for to display an incorrect caller-ID. Just because your phone says company X doesn't mean it's really from them.
3. **Don't pay upfront for a promise** – Many cons will ask for money to begin the process or for you to pay taxes and fees for something you've won, chances are it's a scam. Also be cautious if they request wiring money (like Western Union), reloadable cards, or gift cards since it is harder to get your money back. Of course the caller will say you are getting a great deal and how they are helping you if you pay in this manner.
4. **Take your time** – The caller may also want you to rush you into a rash decision or threaten some consequence if you don't act now. This is also a red flag. You can take the information, do an internet search for the company name with the word scam to see the results, and/or talk to someone you trust to get a second opinion.
5. **Robocalls** – If you get an automated phone call, the best thing you can do is to simply hang-up. Do not press "1" to speak to a person since this will usually simply lead to more calls (since they know that phone number is valid and a human listened and responded). You can and should report these calls to the FTC at https://www.ftccomplaintassistant.gov/#crnt&panel1-1.
6. **How to end the call quickly** – Personally I have had great luck politely but firmly telling them, "No thank you, please take me off your call list." If I have to tell them more than twice I simply hang up, but have only had to do that once in about a decade of using this method.

Reference: https://www.consumer.ftc.gov/articles/0076-phone-scams

Reference: https://www.consumer.ftc.gov/media/video-0028-what-do-if-you-get-robocall

Reference: https://www.consumer.ftc.gov/articles/0060-10-things-you-can-do-avoid-fraud

Children

Younger children can easily become a target or unknowingly make changes to your devices compromising its security. Below are some tips educating and protecting children on the Internet. No matter what, all parents need to do what they feel is right for their particular children since they know them the best.

1. **Get Permission** – Teach your children to ask permission to use the Internet so you are aware. Also monitor their access or keep the device in an open area of the house. You could also implement the rule that the tablet must stay in the living room for example.
2. **Use Software** – There are several browser plug-ins that will block many gambling or other unwanted websites. Also some Internet Service Providers (ISPs) and paid anti-virus packages have options for parental controls.
3. **Safe Searches** – You can also teach your children to surf the web using a kid friendly engine like http://kidrex.org or Google safe search. This will limit Internet search results to ones appropriate for children.
4. **Don't Share Information** – It's never too early to start teaching people to be cautious when sharing personal information online. Seldom (if ever) should a child be putting their name, address, or phone number into any computer.
5. **Encourage Openness** – To me this is the most important item. If you can foster an environment of openness with your child they will be more likely to see you out when something happens or they have questions about something potentially controversial. The most important step in this is not to blame or become angry when they do tell you something they did or saw online.

Reference: https://youtu.be/NqlTOOY9CIo or "5 Tips to Keep Your Child Safe on the Internet"

Fake / Bad Tech Support

Everyone (even experts) needs assistance from someone more knowledgeable in computers or a specific computer area at least. This might be advice on the internet of how to resolve an error or how to reload an operating system when there has been a virus or system error. Unfortunately there are many criminals posing as legitimate tech support services and many people working in the IT field that overestimate their knowledge. Below are some tips to assist in identifying more reputable computer service providers.

1. **Unsolicited Support Calls** – "Windows" will never call to inform you there's a virus on your machine. In fact, "Windows" is not a company name, "Microsoft" is, but they still won't call you. If you want their assistance you must contact them and usually pay $500. Unfortunately, many people fall for this or similar scams and allow hackers into their network simply by going to a website that someone on the phone told them to access. These con-artists will sometimes run a scam for years, each time explaining how hackers got into their system and slowly increasing their support costs upwards of thousands of dollars. Again these individuals are very convincing and slowly build-up a relationship before they start exploiting the victim for money. Please use the tips in these documents to avoid being one of their victims.
2. **IT Freelancers** – Information Technology (IT) is a very broad industry and can be extremely hard to build professional work experience. For this reason, many high school, college students, or people running a side business sell their growing IT services to family, friends, and their community. There is absolutely nothing wrong with this. It builds their experience, encourages entrepreneurs, and can offer IT services to customers far cheaper than many brick and mortar stores. However many of them fall into the trap of believing that they know everything about all fields of IT and that if they can't fix it, no one can.

In one such situation, one extremely knowledgably individual on Macintosh was approached by a customer. The customer had followed advice on an online forum to resolve an issue by deleting his C:\system32 folder (please never do this) on his Windows computer. The customer did it and could no longer boot his computer. He pleaded with this IT individual to retrieve all his family photos and documents. Unfortunately the IT individual wasn't familiar with Windows computers and told the customer nothing could be done and everything was lost. In truth, there was a very simple way to retrieve all of the photo and documents, however by the time this corrected information reached the customer he had already thrown away the computer. If you chose to utilize freelance services like this, ask what their areas of expertise are. No one is an expert in everything, and their answer can help you judge what they might be able to assist with successfully and which they can't. Also don't be afraid to get a second opinion, just to be sure that you're getting the best support as possible.

3. **Brick and Mortar (Traditional) Stores** – There is usually a fair amount of financial overhead with owning and operating a brick and mortar storefront. Most (but not all) of these companies must be reputable to stay in business and still "keep the lights on". However don't assume that the price for one service is the same everywhere and that all IT employees are equally as skilled. I called two different IT service stores in Hampton Roads and asked them for a quote to "reload a computer that had been severely compromised by a professional hacker". The one company explained what they would do (which is what I would also have recommend) and the quote was $198. The second company told me I only needed a cheap $100 service (that I'm familiar with and would not have solved the issue). When I pressed, "what if that doesn't fix it" after a lot of side stepping they alluded to the total price being about $500 or more (which is also what I've heard of other people paying this company). My advice is to shop around and ask other people in the area their experiences with that company. Usually the word gets out quickly about disreputable companies.