Being Hacked

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.

Overview

Hopefully you are reading this in preparation of what might happen, however you also might have been a victim of being hacked. First realize that as a victim of a criminal/hacker (the same as victim of more traditional crimes) there is often a sense of violation and loss of security in addition to possible monetary and data loss. The sections below will not eliminate or compensate for this violation, but might assist in the recovery process and help you identify options available to you.

Unfortunately the Internet is often referred to as the "Modern Day Wild West" and for good reason. The very nature of the borderless interconnectivity of the Internet often makes it difficult or impossible for authorities to work between Counties to prosecute many of these criminals. This is compounded by the complexity and broad scope of IT usually leaving law enforcement unequipped to deal with the quickly changing cyber security landscape.

You can do everything right in protecting yourself and devices from being hacked. This greatly reduces your risk of being hacked but does not eliminate it. Just because you might be hacked doesn't necessarily mean you did anything wrong or were naive. This guide will try to take a generic overview of processes and common options available in these cases.

Terms/Definitions

Ransomware – This is when your computer is infected with a virus that upon boot-up you are prompted with a screen saying your information is encrypted and to access it again you must pay a certain amount of money to the criminals.

Preparation

Backups – One of the most critical steps is to keep your information backed up. This can be to a cloud storage location (using a unique username and password) or better yet an offline backup just as a DVD or jump drive. Be aware that the lifespan of an average DVD in storage is 10 years before it deteriorates and is unusable. With jump drives you ideally want two and to alternate them (one for even month backups and one for odd month backups). It would be painful if the week you went to update your jump drive backup was when you were hacked and they destroyed the jump drive as well. It helps to

get into some routine such as when you pay your mortgage you backup all your new files. This is can be the only safeguard in the case of ransomware.

Protect your devices – Please read the other related articles found at https://www.yorkcounty.gov/IT to patch and protect your devices.

Insurance Coverage – Make a phone call to your insurance provider and ask what computer security items are covered by your current policy, you might be surprised. They will also be able to advise you to what coverage options might be available especially if you don't have the skillset to reload your devices yourself (can cost well over $200).

Authorities

When in doubt you can contact the authorities (local police or sheriff departments) and they can give you the exact information and what they might be able to do to assist. Items like identity theft should be reported immediately. However, at the time of this writing, in York County, Virginia (and most other places), the Sheriff's office will create a report for "computer trespass" or "monetary loss" (such as ransomware but not for other viruses that simply need to be cleaned off the computer). Unfortunately without a lot of additional information and/or a clear local perpetrator most of these items will go unsolved due to a global lack of resources.

It is highly recommended to report all incidents to the Federal Bureau of Investigation Internet Crime Complaint Center (or FBI's IC3). They compile information and when there have been many victims they may pursue the criminals (based again on resources). Many times even if they pursue a criminal you reported you most likely will not be contacted (due to logistics and resources), however they do use the information you provide.

Other resources that might be able to assist with the respective portion is: banking institutions' fraud department and your homeowner's (or similar) insurance company.

Electronic Recovery

Ransomware – Initially ransomware was effective since the criminals that launched this would always provide the unlock keys if the ransom was paid. However since then more criminals have become involved and the chances of getting the unlock key after paying the ransom based on most sources is 50%. If you have your information backed up, most people take their computer to a local computer repair shop to be reinstalled and then restore their documents without paying the ransom. If there are no current backups of the data then it is a more difficult choice that each person must decide for themselves based on the worth of the potentially lost data.

Virus / Malware – Many viruses and malware can be removed by launching an anti-virus program, such as Malwarebytes (free version). However the viruses may have caused unrepairable damage to the computer, usually seen by the computer crashing or locking up. If this is the case, it is usually best to reinstall the computer's operating system or perform a factory reset. All of these tasks a local computer repair shop can assist with. In addition once the anti-virus program cleans the PC there will be a report of the viruses and malware eliminated. Each of these should be researched on the internet to find out

what their purpose was. Be on the lookout for “keylogger”, “data miner”, or other viruses designed to steal your information. If you were infected by some of these you want to follow the “Compromised Information” section as well.

Social Engineering \ Compromised Information – This can be potentially the most extensive and complicated section. A hacker who has access to your computer overnight can run programs to retrieve information that was deleted from when you first purchased your computer (called data mining). In hindsight it is often hard to judge if you overreacted to an incident, however if you underreact the result may be bank accounts being emptied, being hacked again, your identity stolen, or other associated crimes. At the end of the day, you must do what you feel is sufficient and justified to protect yourself and your assets.

1. In the case of social engineering do not speak with them again. You may want to scream and yell at them for taking advantage of you, but you will be alerting them that you are on to them and they may immediately begin using the information they obtained to access your accounts. They are usually much more experienced at abusing the information they collected than you are at defending yourself. Simply immediately and permanently discontinue all communication for this person/organization.
2. Unplug the device from the internet via cable and turn off the Wi-Fi and cellular.
3. If you paid this person via credit card or they had access to your machine/device (including cell phone) that had accessed your bank account: Call your credit card company/financial institution and ask for the “fraud department”. Explain to them what happened and they can advise you to their specific recommendation which may include changing your online login and reissuing you a new credit card number. Be open and honest with them as they are there to assist, you are their customer, and they usually have a lot of experience with these situations.
4. Change your email account password. Many websites allow you to reset your login information by sending you an email, so you want to make sure this is secured as soon as possible.
5. Update other websites you log into from the device such as Facebook, Linked-in, applications, etc. These items are usually the easiest for the criminals to access and are targeted fairly quickly.
6. Check the other devices that connected to that device. For example if the hacked device was your home Windows computer when it was compromised, run a virus scan on any other computers at your home, your phones (connected to your home WiFi), and any other Internet of Things devices. See documentation on “Anti-virus”, “Operating Systems”, and “Software or App Updates”. The last thing you want is for the criminal to still have access.
7. Contact your insurance company. Most insurance companies have various options for “computer coverage”, “Fraud package”, or some items are simply under homeowners insurance or umbrella coverages. Worst case you waste a phone call, best case you might be able to file a claim and have your associated expenses covered. They may have certain criteria specific to the policy that you will need to know sooner rather than later, such as filing a police report, saving receipts of work done to restore the device, etc.

8. Due to the nature of the compromised system in this case it is highly recommended to take your device into a local IT repair shop to have the system wiped and reloaded to make sure all “backdoors” have been removed.