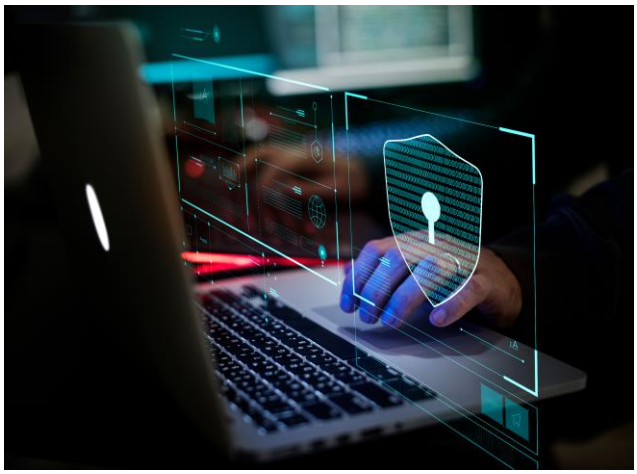
Hackers and What You Can Do About Them



The Problem of Hacking

Although the internet appears to be a viable resource, this era of instant answers and social media does not come without its risks. Imagine your Google account being shut down for two days or all of your information being stolen. Or, the website you spent months creating is now a hot mess. The problem of hackers looking for people's personal information and money is an unfortunate yet common problem on the internet today. Fortunately, we are becoming increasingly knowledgeable about what causes and how to prevent hacking. The more we can become educated about this problem, the higher the chance of avoiding it. Really, the safest way to do things is the old-fashioned way. However, in this age, awareness goes a long way.

Top Protection is Needed for Your Protection

Here's what to know!

Hackers can easily install viruses onto your computer. They can load desktop files that, once opened, can steal personal information from your computer. One type of such virus is the zip file virus, which contains poisonous information. These types of files can easily be put on computers. However, they will look suspicious. Another file is called Home. This file is actually a virus. These two types of files look normal, almost like Window files. However, you can recognize them as suspicious because they are scattered around the computer and look immediately out of place.

Even with a firewall, websites can still be hacked. Firewalls are not full protection, and, in fact, a website can be repeatedly hacked with a firewall by using malware to corrupt files on website.

How hackers can access your personal information:

- They are aware of when you are on social media by the IP number and can find you on the web
- They can clone friends and family and get information to send messages via Facebook
- Hackers can install phone apps which can take your personal information, including personal texts
- Hackers can steal everything on your computer by the apps and files they install

What harm hackers may create:

- They can load desktop virus files onto your computer
- They can take down YouTube and Google by a phone number and email combination
- They can knock down YouTube views and Subscribers
- They can knock down likes and followers on Facebook, Instagram, and Twitter
- They can control texts – text virus can steal important information on your phone
- They can gain full control of your personal information
- They can shut down your internet service
- They can prevent emails from going out (and they know when you are emailing)
- They can freeze and time out screens
- They can lock you out
- They can freeze a screen shot on your phone, preventing you from receiving emails without restarting your phone
- They can overload a server with information and causes a website to shut down (DDOS)
- They can change the apps on a computer
- They can interfere with downloading
- They can send daily emails, which if opened can create a virus
- They can interfere with downloading
- Your email can be interfered with and can show an error
- They can send corrupt files to your computer through the internet and through IP address
- They can create continuous malware difficulties on websites
- They can control your computer file
- They can steal or delete files from your folder
- While driving, hackers can flash the screen from the security screen to Google maps, causing a safety hazard
- They can control Google Play and stop you from buying and downloading an app
- They can send notifications about Google apps they control
- They can put your website into technical difficulties, not letting web designers repair the damage the hackers have done to your website

- They can change app setting so that a Kaspersky Tech or Security Tech can't see while on your computer checking for service
- They can create a website with a similar domain name to yours to throw off your website security and Google search, thus protecting the hackers' page while making your website invisible on Google search engines and vulnerable to website attacks

Be aware of these phone apps which take your personal information:

- Moto
- Easy Spy
- Surepoint Spy
- Phonespector
- Highster Mobile
- Auto Forward Spy,
- XNSpY
- mSpy
- SteatlhGenie
- iSpyoo
- MobiSTeath
- Spyzie
- Duplicate apps such as a "Files app" seen twice

How to protect yourself from hackers:

- Never give out personal information
- Keep web cameras and microphone off to prevent being followed by hackers and scammers
- ***Be aware of pop-up windows on your computer (malware) - Malware virus can remove almost everything from your computer***
- Do not accept apps or files from anyone
- Remove files on your computer which are corrupted by hackers
- Do not accept or open pop-up notification windows on your computer (even if you think its part of your security system)
- Install a scam shield on your phone
- Install security protection on your computer and phone
- Avoid paying bills online
- Avoid keeping debit bank card information online

- Make adjustments on your phone to stop FAKE alerts
- Don’t use a web camera
- Avoid Facebook cloning
- Must watch a crime prevention guide such as the Crime Prevention Guy’s YouTube videos an officer in Texas
- Put Kaspersky lab support and total security on your phone and computer - will alert you when camera or microphone is on
- Don’t give out telephone number and email at same time
- Delete spam messages that may contain viruses
- Back up your website daily
- Fully scan your computer for viruses
- Google an app to see if it is spam
- Pay for VPN, which can change your IP computer address to anywhere you want
- Send hard copies of photos to your family and friends, rather than through the computer
- Keep record of all your scammed phone calls - your attorney can take that information and turn into a legal attempt to get scammers/hackers to pay for stress and damage, and this could even go to trial if they don't settle it outside of court

What to look out for:

- A loud computer – a computer will make a loud revving noise when a virus or malware has been installed
- Deceivingly serious messages that come across your phone with the warning “FAKE”
- Absence of your Google account
- Missing text messages – they can also send a text with a virus
- Calls are disconnected midway through the call
- Your storage apps are missing
- A Google meeting keeps appearing on your computer asking you to join in meeting (this is a hacker / scammer)
- A swipe of your phone reveals a camera ready to take your picture
- Your phone or computer settings being controlled, such as: brightness, sound, email cursor, and pop-up window, resizing
- A security engineer (hacker) notices your website has vulnerability, then asks you if he/she the security engineer can fix it for a sum of money
- Turning off your computer once your computer has just booted up
- Your email being interfered with

Actions you can take if hacked:

- Call the state police, who can let you know if you if you've been scammed
- Norton Security and engineers are waiting to help you if you think you have a problem with hacking on your computer. They will come online and help you resolve issues and let you know if you've been scammed
- Install Kaspersky lab on your device (mentioned also in how to protect yourself)
- Change phone number or email and password if you think you have been hacked
- If a cell phone has been hacked, have a friend set up a new Google account with a new email and new phone number from your phone company – this will disallow the hackers into your Google account and phone
- There steps to cancel and remove Google meetings that appear on your computer
- Apps are constantly changing. Check phone company for more information
- Contact Microsoft – check your windows security
- There are steps to remove your camera from phone – check with your security protection
- Ask provider to change IP address on phone and computer
- Contact your Internet supplier and phone carrier to change IP addresses to supply you IP addresses that will protect you from hackers/scammers
- Contact your police department– you will need IP addresses for police detectives to track scammers. FBI report can be filled out if a business has lost money because of hackers or scammer
- Reset your cell phone completely

MA Cyber Computer Crime Laws:

- Stalking MGL c. 265 s.43
- Child Enticement & Exploitation
- MGL c. 265 s. 26C
- Hate Crimes, Racism, & Hate Websites MGL c. 22C s. 32
- Massachusetts Laws Governing Copyright Infringement MGL c. 266 s. 143A, 143C and 143E
- Whoever violates any provision of section 143A to section 143C, inclusive, shall be punished!
- Illegal Purchases MGL c. 266 s. 37E

Of particular note is the MGL c. 265 Section 43 as detailed below.:

(a) Whoever (1) willfully and maliciously engages in a knowing pattern of conduct or series of acts over a period of time directed at a specific person which seriously alarms or annoys that person and would cause a reasonable person to suffer substantial emotional distress, and (2) makes a threat with the intent to place the person in imminent fear of death or bodily injury, shall

be guilty of the crime of stalking and shall be punished by imprisonment in the state prison for not more than 5 years

The Federal Cyber Computer Crime Law

The Computer Fraud and Abuse Act (CFAA), 18 U.S.C. 1030

https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf
The Computer Fraud and Abuse Act (CFAA) [18 U.S.C. Section 1030] makes it illegal for anyone to distribute computer code or place it in the stream of commerce if they intend to cause either damage or economic loss. The CFAA focuses on a code's damage to computer systems and the attendant economic losses, and it provides criminal penalties for either knowingly or recklessly releasing a computer virus into computers used in interstate commerce. Someone convicted under the CFAA could face a prison sentence as long as 20 years and a fine of up to $250,000.

Pick up the phone and call! Don't take a chance of this happening to you!

Updated 2/23/2021

Cybercrime can affect anyone! If you experience any of the crimes/abusive acts as stated on this document or if you would like more information, immediately contact or search any of the agencies below. Be sure to make copies of everything for yourself. Keep Your Community Safe, Make the Right Choice! Report Cyber Computer Crimes!

General Cyber crime information

General Cyber crime and fraud information:

https://fraudsupport.org/

The Crime Prevention Guy! A Texas Police Officer!

https://www.youtube.com/channel/UCKk2UYqi4fy7qEPlVFX3Bcg

Forward unsolicited e-mail offers or spam:

spam@use.gov

To determine whether your website is safe:

https://www.websitebuilderexpert.com/website-builders/comparisons/squarespace-vs-wordpress/

To improve your Google search (SEO) for your Website:

https://search.google.com/search-cons...

To learn how to reduce spam:

https://www.consumer.ftc.gov/articles/0038-spam

US Computer Crimes Hotline:

Call: 877-438-4338

https://staysafeonline.org/contact/

For problems with Google and/or YouTube:

Fax: 650-253-0001

Concerns About Massachusetts Cyber Crimes:

MA Attorney General Office Hotline:
Call: 617-727-2200
https://drive.google.com/file/d/1DQjK0bjGX963Uw9_uOaROjiS-mtBXkhD/view

MA Cyber Crime Unit Hotline:
Call state police: 774-462-3750

Massachusetts Computer/Cyber Crimes M.G.L. c. 265 s. 43

https://malegislature.gov/Laws/GeneralLaws/PartIV/TitleI/Chapter265/section43

MA Forensic Computer Crime Center
Call State Police: 978-451-3300

Information on Cyber crimes

https://www.mass.gov/info-details/cyber-crimes

The Attorney General's Cyber Crimes Division

https://www.mass.gov/the-attorney-generals-cyber-crimes-division

MA Criminal Court Proceedings - Court
https://www.mass.gov/how-to/file-a-criminal-complaint

Concerns about Federal Cyber Crimes

US Cyber Crime Center:
Email info@dc3.mil

FBI Hotline:
Call 857-386-2000

FBI Internet Crime Complaint Center:

FBI IC3 Complaint Referral Form online:

https://complaint.ic3.gov/default.aspx

US Criminal Court – US Court

https://www.uscourts.gov/sites/default/files/ao091.pdf

Consumer Protection provided by "We Are Electricians"

P. O. Box 541445 Waltham, MA 02454-1445

www.maelectricalcontinuingeducation.com