THE ESSENTIAL GUIDE TO ONLINE SECURITY

A Comprehensive Collection of Best Practices to Keep You Safe Online

Author: Geoffrey Vaughan
Contributing Editors: Zak Dehlawi, Anna Stenwick, Lauren Yanko

Introduction

Often with security and privacy concerns there exist trade-offs with usability and complexity. The most secure user is often the one who doesn't use the Internet, but if you would like to climb out from under your rock to join the rest of us on the Internet, this guide is here to help you. Getting to a point where you can be reasonably confident in your personal security and privacy online can take a lot of effort, due diligence, and technical vigilance.

All of the items in this guide can be overwhelming. Don't treat these items as hard and fast rules to tackle all at once, rather over time do your best to improve your overall personal security and privacy by implementing and trying out more of these practices. Once you have tried many of them out, you can then decide for yourself what your security and privacy needs are compared to the relative inconvenience and acceptance for the listed threats.

Table of Contents

SECURITY INNOVATION

PASSWORD SAFETY

Passwords are probably one of the weakest parts of the Internet. They can be guessed, stolen, stored incorrectly, overused in repetition, found written next to computers, forcibly reset, and much more. Unfortunately, better and easier authentication methods aren't widely deployed, so we have to do our best to protect any passwords we create.

Creating a Password

First of all, whenever you see "password," you should think passphrase. Gone are the days where you can use one word as a passphrase.

PASSPHRASES SHOULD:

- Be 10-20 Characters long
- Be a combination of upper and lower case letters
- Include special characters and numbers (space bar and tab often counts)
- Be something you can remember (sometimes)
- Not be used on other sites (you shouldn't re-use the same password to access your email, banking, etc.)
- Be changed / rotated frequently (every 3-6 months). Usually, whenever a big data breach happens it's a good time to think about changing your passwords, even if the breach doesn't affect certain applications.

MyR3dSt@p!eR_25

WATCH: Password Security in 2 Minutes

Three popular password managers include:

1. **LAST PASS**
2. **1PASSWORD**
3. **KEEPASS**

Password Managers

It is very difficult to remember dozens of passwords and usernames for online accounts. As a result, people have reverted to choosing weaker passwords and using the same password across multiple sites. When using weak passwords, users open themselves up to their accounts being compromised by attackers who will attempt to guess their password. If one of the sites you use is hacked and all the usernames and passwords are revealed, many malicious users will try those usernames and passwords across multiple popular sites (banks, social media, email providers, etc.). If you used the same password everywhere all of your accounts could be in jeopardy.

Password managers allow you to use unique, strong, randomly generated passwords across a variety of accounts and store them securely in an encrypted database on your machine or “in the cloud.” This database should be encrypted with a strong passphrase and not shared with anyone. One drawback is that this creates a central repository of all your passwords. This is often seen as a trade-off between using a password manager and having to remember multiple weaker passwords across many sites. Given the central repository of passwords that could unlock all of your accounts, there is an additional risk of using a password manager that uploads the encrypted database with a remote server and shares your passwords with all your devices. If you are more risk adverse, look for a password manager that does not sync remotely or disable this feature.

Two-Factor Authentication

If an attacker gains access to your password through either malware or just plain guessing, they can log into your online accounts containing sensitive data. Two-factor authentication, sometimes known as 2FA, introduces another layer security that a malicious user needs to bypass.

There are three main types of authentication mechanisms in use today: what you know (passwords, usernames, SIN/SSN number); what you have (keys, access badges, your cell phone); and what you are (biometrics). Two, or multi, factor authentication refers to using two or more of these methods to prove you are who you claim to be. Wherever possible, you should enable 2FA for all of your online accounts.

The most common 2FA method is your password plus a special verification code sent to your cell phone. That way if you know your password and have your cell phone, only you will be permitted to log into the application.

Facebook, Google, and Twitter all support 2FA:

FACEBOOK LOGIN APPROVALS:

https://www.facebook.com/notes/facebook-engineering/introducing-login-approvals/10150172618258920

GOOGLE 2FA:

https://www.google.ca/landing/2step/

TWITTER LOGIN VERIFICATION:

https://blog.twitter.com/2013/getting-started-with-login-verification

Start by enabling 2FA on these sites and then expand from there. To view a fairly comprehensive list of sites which support 2FA, check out https://twofactorauth.org/

MOBILE SAFETY

Mobile devices have become a large part of our everyday lives. We are never more than an arms-length away from our phones. Many of us also use our phones for work purposes as well as personal use, which then puts private work information at risk as well. Unfortunately, many of us don't protect our mobile devices as best we can, leaving us vulnerable to an attack.

Android Safety

With many diverse offerings of Android devices and many variations in the operating system, the range of potential attacks against Android devices is quite broad. Often security patches are released but users do not install the updates. Cell phone providers and carriers are also in the habit of deploying custom branded versions of operating systems with their own potentially vulnerable software preloaded, or failing to update custom branded versions with new security patches. Users also need to protect themselves against a full range of threats that could compromise their personal data; from mass surveillance, rogue applications, and excessive data collection the list of threats is quite long.

BEST PRACTICES FOR ANDROID DEVICE SAFETY:

- ✓ Keep your phone up to date.
- ✓ Use a strong password or pattern.
- ✓ Enable full disk encryption.
- ✓ Ensure USB Debugging is off.
- ✓ Ensure developer mode is not enabled.
- ✓ Do not root your device.
- ✓ Where possible use a Nexus device as they are updated regularly.
- ✓ Back up your device locally regularly.
- ✓ Ensure that GPS features are properly configured to not disclose your location.

Chances are the operating system that came with your phone is loaded with bloatware (useless marketing apps that perpetuate the cell carriers' brand) and vulnerabilities from your cell phone service provider.

For more advanced users, it is strongly recommended that you remove the default installed operating system and use a trusted OS that is regularly updated. Where possible use a Nexus device with its stock OS or use official builds of Cyanogen Mod (http://www.cyanogenmod.org/). Replacing your device OS can be an involved process and could damage your phone or void your warranty, so tread carefully.

▶ **WATCH:** Mobile Security in 2 Minutes

iOS Safety

For most people, their mobile device is attached to their hip or glued to their hands for every waking hour of the day (and then some). In some ways it stores more personal information about you than your computer including: images, location, contacts and an active connection to all your social media accounts. It is the key to your digital life. How can users best protect their digital lives if their device is lost or stolen? Additionally, users need to protect themselves against a full range of threats that could compromise their personal data; from mass surveillance, rogue applications, excessive data collection, etc. Although Android devices are targeted more frequently, iOS devices are at risk as well.

TO PROTECT YOUR IOS DEVICE:

- ✓ Use a secure lock-screen password, if you use your fingerprint to unlock, you can set a much longer pass-phrase for use on boot.
- ✓ Enable Find My Phone and test it out with another Apple device (or online) before you lose your phone.
- ✓ Change the default Wireless Hotspot password.
- ✓ Keep your device up to date.
- ✓ Review each installed application's requested features and limit them as much as possible. They can always be re-enabled on demand.
- ✓ Enable auto-lock using a short time-out.
- ✓ Do not Jailbreak any device you use regularly.
- ✓ Do not backup sensitive data to the iCloud service. If you are unsure of this, completely disable iCloud. You can back up a complete image of your device locally using iTunes. Store this backup securely.
- ✓ Ensure that GPS features are properly configured to not disclose your location, and applications do not have location permissions.

Text Messaging

The SMS protocol is another protocol where all data is sent in plain-text (unencrypted) and could be read by anyone who can view it in transit. This includes the wireless cell providers of both the sender and receiver, as well as any cell towers the either phone is connected to. Apple's iMessaging is a little different, they send the messages over an encrypted channel and claim that not even they can read messages, although this claim has not be validated. There are also a number of government agencies attempting to subpoena Apple to reveal this information, and laws have been proposed to force vendors to put in security backdoors for governments.

> For sensitive SMS conversations, some chat applications should be avoided; particularly those with a history of breaches/vulnerabilities, or that ask for excessive permissions to operate, such as **Snapchat** and **Whatsapp**.

To secure text messages, **make use of 3rd party applications** to communicate securely with friends such as **TEXTSECURE** for Android and **SIGNAL** for iOS. Although their security can't be guaranteed, it is better than sending messages in plain-text.

GPS

Your phone or tablet can be a great weakness in personal security if configured incorrectly. Malicious applications can use the device's GPS to track your location. Even non-malicious applications might be configured to post your location to social media. In addition, the camera application might enable GPS tagging of all images you publish. This means any image you share would reveal your exact location.

Where possible, disable the GPS and restrict individual apps from accessing the GPS location feature of your phone. This will limit the risk associated with malicious attacks regarding your location.

DEVICE SAFETY

Your desktop or laptop computer is a prime target for malicious users. If they're able to compromise your device they can steal your passwords, files, and other sensitive data, as well as bypassing many of the security controls you might have put in place. Malicious users often target Windows PC users, but have been known to target Mac users as well.

PC Safety

For Windows PCs, there are many security features that can be configured and modified in various configurations to affect the security posture of your system.

ARE YOU FOLLOWING THESE BEST PRACTICES?

□ I'm using the latest version of Windows. (Microsoft tends to include more security features with each iteration.)

□ I turned on Automatic Updates and ensure my computer is regularly updated to prevent known attacks on Windows from affecting me.

□ I ensured that the Firewall was enabled.

□ I use an antivirus application.*

□ I disabled the windows key-logger (if using Windows 10)!

□ I disable cloud features when I'm concerned with uploading sensitive data to the cloud.

□ I scheduled regular system restore points and perform backups to encrypted external drives.

*Truthfully, antivirus applications are way overrated. They are just a small part of your overall security. For most users, applying regular patches will do more for your security posture then an antivirus application, but antivirus applications can catch and prevent known malware.

Mac Safety

Windows continues to be the dominant operating system for laptop and desktop computers, but a significant number of users use Macs and the OS X operating system. In the past, people believed that Macs could not get viruses, but recently more malware has appeared targeting OS X. You are also open to many of the other threats discussed in this document.

HOW ARE YOU KEEPING YOUR MAC SAFE?

□ I only install trusted applications from the Mac App Store, including enabling Gatekeeper.

□ I ensured that the Firewall was enabled.

□ I disable iCloud storage when I'm concerned with uploading sensitive data to the cloud, but I have "Find my Mac" enabled.*

□ I enabled a strong lock screen password.

□ I am wary of applications that ask for my admin password or need administrator permissions to run.

□ I disabled the guest account.

□ I scheduled regular Time Machine backups to an encrypted external drive. (Time Machine backs up your data as well as system files.)

*The "Find my Mac" feature takes some tinkering with settings to get it right.
Test the "Find my Mac" feature before you need it.

Backups

Backups can be a life saver. If your device is ever lost, stolen, corrupted, or compromised in any way you can quickly revert to a backup. However, depending on your backup methodology you can expose yourself to additional risk by opening your backups to compromise.

Here are two options for backing up data:

OPTION 1

Remote backups built into your OS such as Apple iCloud or Microsoft OneDrive are often the easiest way to back up your computer and data; however, they can also be the most vulnerable. Consider the recent iCloud incident where private celebrity images were stolen from Apple iCloud.

OPTION 2

If the data is sensitive in nature, all backups should be stored fully encrypted, either locally or remotely. For local backups, an encrypted external hard drive can be used specifically for the purpose of storing backups. However, you run the risk of losing your local device. For remote backups, data should be encrypted before uploading to third party servers and not relying on the third party to handle the encryption.

BEST PRACTICES FOR BACKING UP DATA:

- Fully encrypt any backups with a strong passphrase.
- Store sensitive backups on an external drive that only you can access.
- Encrypt data locally before storing it remotely.
- Test your backup system periodically to ensure it works.
- Where possible, backup your full system configuration in addition to all of your data.
- Windows System Restore is often not sufficient for backup purposes as malware often attempts to wipe it and if the hard drive fails the backups are lost.

Local Storage

If you have ever lost or had a device stolen, you know it can be pretty devastating. What's worse is if the data is not encrypted. Not only will you have lost the data, but it could also be in the hands of someone else.

Full disk encryption, with a strong passphrase, should be used anywhere sensitive data is stored, whether on a desktop computer, laptop, mobile device, USB drive, or memory card.

Updates

Software vendors frequently release new updates for software after vulnerabilities have been discovered and fixed. Those who don't update their software and devices will still be vulnerable. Malicious users are always on the lookout for recently updated software in order to identify and exploit the vulnerabilities the patches fix. In most cases, keeping your software up-to-date can be more valuable and a better security decision than using an antivirus application, although you should also do that.

Update your software regularly (weekly would be ideal).

1. **BROWSERS**
2. **OPERATING SYSTEMS**
3. **PHONES**
4. **APPS**
5. **ALL OTHER SOFTWARE YOU DEPEND ON**

Set software, such as Windows, to update automatically.

SECURE COMMUNICATIONS

One of the most common reasons we use laptops and mobile devices is to communicate with each other. Whether this be family, friends, or colleagues at work, using these devices helps us stay in touch and get the job done.

Email

When sending an email, there are no guarantees the data is secure or encrypted completely from the sender to the receiver. Often your connection to your email provider will be secured but after that you have no way of knowing if your email will be read or stored at some point before it reaches its destination. For this reason, any sensitive information should not be transmitted over email without being properly encrypted.

THE EASY SOLUTION:

If you have a sensitive file that you want to send to someone, consider compressing it into an archive file (.zip or .rar for example) then set a strong passphrase to encrypt it. This is often done using the advanced settings of your archiving application. Then, email the recipient the file and send them the password via another means. NOT OVER EMAIL. Consider using SMS or calling them to give them the password.

▶ **WATCH:** Email Security in 2 Minutes

THE MORE DIFFICULT SOLUTION:

Strong email security usually requires some technical forethought from the company or parties involved. Two leading solutions are PGP/GPG and SMIME.

For details on PGP/GPG encryption see this guide on OpenPGP for beginners: http://zacharyvoase.com/2009/08/20/openpgp/

For details on SMIME please see this guide: http://www.esecurityplanet.com/views/article.php/3910181/Simple-Steps-to-Securing-Email-with-SMIME.htm

Social Engineering

Social Engineering is a broad topic in security where an attacker will attempt to gain information or get you to perform an action by just talking to you. Often this is done either in person, over the phone, or via email, but on every platform of the Internet there is someone trying to run some sort of social engineering scam against you.

TRUTHS ABOUT SOCIAL ENGINEERING:

- ! If it sounds too good to be true it probably is.
- ! No one is trying to send you money, not even a Nigerian prince.
- ! Your bank would never call/email/ask you for your information. If it really is your bank ask them to prove it (i.e. What's my balance?).
- ! A company would never call you to provide technical support.
- ! Nobody can know that your machine is infected with a virus, don't trust anyone trying to tell you that they can fix it over the phone.

PROTECT YOURSELF FROM SOCIAL ENGINEERING:

- ✓ Web search the caller-id number from the person calling you.
- ✓ Don't open attachments or click links from anyone you don't know.
- ✓ Hover over an email address/link to ensure it matches what it claims.
- ✓ Attempt to verify the identity of anyone who contacts you.
- ✓ Do not give out any personal information.
  - Do not let anyone into your home.
  - Do not fall victim to pressure tactics. Attackers will try to make you feel guilty for not helping them.

Social Media

Social media and dating sites can be loaded with people looking to misuse your personal information. It can also be a great source for attackers to gather information about you to attack your other services (banking, email, etc.). As a social media user, you need to watch out for fake accounts trying to connect with you, corporations and governments running mass data collection to track or advertise to you, identity thieves looking for weak victims, and real world thieves waiting for you to post that you are out of town so you can be burgled.

PROTECT YOURSELF ON SOCIAL MEDIA WEBSITES:

✓ If security and privacy is important to you, think very carefully about each and every post you make and what you choose to share.

✓ Review the privacy settings for all your social media accounts to ensure you are only sharing information to the people you want. “Friends of Friends” is a very large group of strangers.

✓ Avoid the temptation to post location information or broadcast vacation plans. When possible, post vacation pictures at the end of the experience or not at all.

✓ Dating accounts can likewise contain more sensitive information than your banking information so be sure to protect them as such.

✓ Avoid using the GPS tagging feature in applications and image posts.

✓ Ensure that the pictures you post do not contain additional identifying information such as house addresses, license plates, birth dates, SSNs, ID numbers, etc.

✓ Log out of and clear browsing history on shared computers. Alternatively, use “Incognito” or “InPrivate” browser modes and explicitly log out every time.

GET OTR MESSAGING:

1. Download the chat client (Pidgin or Adium)
2. Connect your desired accounts (Google Hangouts, etc.)
3. Install the OTR plugin
4. Enable OTR and generate a private key/fingerprint
5. Enable force encryption on all conversations

Chat

By using 3rd party chat services such as Skype, Google Hangouts, Facebook Messenger, Apple's iMessage, and countless others, you open yourself up to having all of your private communications stored on that system's server indefinitely. There have also been many attempts (successful and unsuccessful) by governments to gain access to this data via court orders or by forcing companies to install backdoor access. Additionally, if any of these chat applications gets hacked, which happens often, all of your conversations could be exposed.

Off-The-Record (OTR) Messaging is an encryption library that plugs into popular chat clients: Adium for Mac, or Pidgin for Windows. Adium and Pidgin support multiple chat protocols. OTR requires both parties to install the plugin to communicate securely.

NOTE: OTR may not be easily available for Apple's iMessage. They do reportedly do their own end-to-end encryption; however it is entirely within Apple's control, which may be subject to being subpoenaed or subject to mass surveillance. For sensitive content, it is recommended that other methods of encryption be used instead of iMessage.

TRAVEL SAFETY

There are all kinds of additional dangers to be concerned with while traveling and accessing your remote files/accounts. You need to be concerned about all areas of security and take extra care in a few close areas.

Border Crossing Threat

(THIS IS NOT LEGAL ADVICE)

If you intend to cross a border with a device that contains sensitive or personal information, recognize that in most countries the border officials do have authorization to search and seize anything that enters the country. This includes cell phones and laptops. There have been a few cases that argue this point a bit but it usually applies to individuals re-entering their own country. As a foreigner entering another country, your devices, generally speaking, don't have very many rights to exemption from search.

When crossing a border, fully encrypt all device's local storage with a strong passphrase. Then, completely turn off your device. This will make the device resilient to many other types of attack. If a border official seizes your device in this case, it will be difficult for them to break the encryption. If they wish to search the device, you will have to be present to reveal the encryption passphrase.

NOTE: If you are asked to turn over your passphrase you will have to weigh the choice between your potential refused entry into the country and the risk of having that data turned over.

Shared WiFi Threat

By norm, WiFi networks from hotels or even airports are among some of the worst wireless networks around for privacy and security. In most cases, anyone on these networks can see everyone else's traffic.

ARE YOU FOLLOWING THESE BEST PRACTICES?

- □ I'm using these networks sparingly and not for any sensitive activity (i.e. banking, social media accounts, email).
- □ As an alternative, I'm using my cellular data provider (although it is often expensive).
- □ Where possible, I use a VPN connection to encrypt all my traffic back to my home country/employer.
- □ I am diligent to ensure all traffic is transmitted over a secure channel.

Kiosk Computer Threats

It's common for hotels to put kiosk style computers in lobbies or around the hotel for customers to access. These computers are often poorly managed, cache all traffic history, and have additional monitoring software installed on them.

IT'S NOT SAFE TO PERFORM THESE ACTIONS ON A KIOSK COMPUTER:

- Logging in to anything (banking, social media, email, ANYTHING)
- Purchasing anything, this includes booking excursions online
- Posting any personal information
- Uploading pictures

YOU MAY BE OK TO PERFORM THESE ACTIONS:

- Looking for a place to have dinner
- Printing your boarding pass (if you can do it without using email)
- Visiting Facebook/Twitter/Instagram to see if the last kiosk user is still logged in and kindly log them out

You may also want to consider using Tor if your security and privacy needs are great. It's also recommended to wait until you get home to post pictures onto social media.

Wireless Network Safety

If you connect to the "Starbucks" wireless network or any other untrusted WiFi access points, all of your traffic could be intercepted. Anyone else on the network is likely able to also view your traffic.

IN ORDER TO PROTECT YOUR INFORMATION:

- Turn off "Automatically connect to WiFi" on your laptop(s), tablet(s), phone(s), and any other devices, especially while traveling.
- DON'T check email, do bank transactions, or access social media accounts on any public or untrusted access point without a VPN.
- If the properties of the WiFi access point say it's secured by WEP, it is actually not secure and should not be trusted.

Using a VPN

While traveling or making use of untrusted WiFi hotspots, all of your traffic is more likely to be subject to interception. If you plan on accessing your email, banking, or social media abroad this might leave your accounts susceptible to being compromised. Mass surveillance by governmental entities can also be a concern and your sensitive data can be swept and stored indefinitely.

A VPN or Virtual Private Network is the process of logically placing your computer into another network. Often people will use a VPN to take their work laptop home and then have it virtually connect to the office. This would make it appear as if your work laptop is sitting in your office, when it is really in your house. This usually means while you are connected to the VPN, all of your traffic will appear to other servers like it is coming from your employer and not from your house.

WARNING: In some areas of the world using a VPN will get you a not so pleasant visit from authorities. Research the laws/regulations of your particular country before using a VPN.

THE EASY SOLUTION

If you are using your employer's device, you likely already have the infrastructure in place to connect back to your office. Make use of this to ensure all your data is encrypted in transit and your accounts will be better protected. However, keep in mind that now your employer may be able to intercept and eavesdrop on all of your traffic. Don't do anything that not's safe for work on your employer's network.

THE MODEST SOLUTION

For a small monthly fee, there are many VPN service providers that will allow you to connect to their network and tunnel all your traffic through them. This would protect you from most risks while traveling or using untrusted WiFi access points. The problem with this approach however, is how do you trust the VPN provider? This can be a difficult question to answer and it only comes after you do your homework and research all the different connection options.

THE HARD SOLUTION

Consider using the Tor Network to establish your VPN connection. Truthfully, it's not that difficult. It just takes reading a few of the getting started guides and testing it out to ensure that it's working correctly before you put your life on the line.

Using Tor

If you are deeply concerned about your privacy and security online or are in an area that heavily monitors Internet activity, the best viable solution is to use Tor. Tor really serves two purpose, it provide users with an anonymized VPN service, where traffic is routed through many servers before reaching its destination. Secondly, it provides access to part of the "deep web" or hidden Internet servers through what are referred to as ".onion" sites.

TO USE TOR:

1. Test Tor out before you travel or need it to ensure it works correctly.
2. The easiest method to use Tor is via the Tor Browser. Check Tor every time before you begin using it to ensure that it is up to date!
3. Don't connect to personal email accounts or social media when using Tor as it will deanonymize you.
4. Consider using a VPN in conjunction with TOR. It is a little more complicated to setup but it increases security drastically.

INTERNET SAFETY

General Internet safety can go a long way in protecting your private data and other information. Whether it's educating younger children about the risks associated with using the Internet or understanding how browsers store your data, proper Internet safety can prevent an online attack.

Browsers

Your browser is where you interact with the Internet. At some point or another all of your personal information goes through your browser. Not all browsers are created equal, and this is especially true from a security perspective.

BEST PRACTICES FOR BROWSER SAFETY:

- ✓ Use a modern web browser that is always completely up to date. Chrome or Firefox would be preferable.
- ✓ Always log out of any online service after you are done.
- ✓ Always ensure that SSL/TLS encryption is enabled on all sites you are logged into as well as on those where you are submitting any personal information (look for the green padlock next to the URL).
- ✓ Use an ad-blocker to help reduce malicious ads.
- ✓ If you are on a shared or public computer, use the incognito or private browsing mode to avoid sensitive data being stored locally.
- ✓ Regularly check to make sure no additional browser extension or add-ons have been installed. For Chrome, type chrome://extensions into the address bar. For Firefox, type about:support in the address bar.
- ✓ Limit the number of browser extensions you use and only install from trusted sources (i.e. the app extension markets for Chrome or Firefox).

SSL (Secure Sockets Layer)

When submitting data to any website, the manner in which it is sent can either be in plain-text (unencrypted) or encrypted. This encryption method is often referred to as SSL, TLS, or HTTPS. When your data is sent to a website it is often sent through multiple routing points before it reaches its final destination. If that data is sent in plain-text, it can be stored/viewed by anyone who can "tap the line" or eavesdrop on the communication channel, such as public WiFi.

Get in the habit of looking at the URL bar for every site you visit. Different browsers represent SSL a little differently, but they all generally use a green padlock indicating that the communication channel is secure. For a comparison of different browsers and their way of representing SSL/TLS/HTTPS, visit www.expeditedssl.com.

CAUTION: If you ever get a security warning telling you the communication channel is not secure, do not proceed further and notify the site owner if possible.

Talking to Your Children about Online Safety

There is a long list of dangers on the Internet your children could fall victim too. These threats include:

- ! Bullying
- ! Child predators
- ! Seeing adult content at too young of an age
- ! Addiction to computer/video games
- ! Advertising enticing your kids to spend money (your money)
- ! All the other threats mentioned in this document

Admittedly, the above list is quite terrifying. On that fear alone, you could install a long list of tools and software to spy on your children's online activity, firewalls to restrict access to sites, and apps to install on their phones to track their movement, read all their text messages, and turn their mic on when they are at parties. These draconian measures however, often push your children away from you and create an adversarial relationship between you and your children. The best strategy to keep your children safe online is to talk to them regularly about their online activity. There are many different conversations to be had with your children about the dangers online and as a parent, you will need to decide for your children when the best time is to have these various conversations.

TO HELP PROTECT CHILDREN ONLINE:

- ✓ Try to keep computers in common spaces of your house.
- ✓ Recommend that your children only connect/communicate with friends they have met in person. Review their friends list with them.
- ✓ Educate your children on privacy settings and review with them for their devices, apps, and online accounts.

TO HELP PROTECT CHILDREN ONLINE (CON'T):

- ✓ Consider a firewall, filter, or parental controls on the web browser, especially for young children who may accidentally search or browse to adult content.
- ✓ Have a conversation about what to share and what not to share. For most children, try and reign in the "share everything" attitude and review any content posted publicly.
- ✓ It's alright to ask that your children connect with you on their social media accounts but don't abuse the privilege by embarrassing them and commenting on every post they make.

If your child is being bullied, whether it is at school or online, it can be quite difficult to deal with. Online bullying can be quite hurtful, the perceived impact and reach of a comment can be quite broad and damaging. All social networks have policies to remove offensive posts, obviously the quicker you can address those posts the better. Social networks also have block features but that may mean the conversation will continue without your ability to track and document it.

When trying to resolve and correct the behavior of a bully by approaching the school, police, or other parents, often the person who documents the most evidence has the strongest case. Take notes and screen captures of every interaction and when you have enough evidence to take action do so.

The worst thing you can do in any case of online bullying is fan the flames. It is better to say nothing then to respond to a bully online. If you are going to post anything at all simply post "This comment is unwanted and inappropriate." After which time if the bully continues to respond it is the very definition of harassment. If you or your child has expressed their discontent with the actions of a bully, and it continues, you have a much stronger case.

LEARN MORE

NeedHelpNow.ca - Great new site with resources for parents and children on keeping safe online.