Digital Hygiene

Digital hygiene this isn't about electric toothbrushes and flossing devices. It's about keeping your digital devices, accounts, personal information, files and access secure. You do that by using good security practices, using the right passwords and keeping them private and keeping an eye on your reputation online and off.

Think of digital hygiene as digital self-defense. Most digital problems can be avoided if you prepare in advance. It is much harder to stop cyberabuse once it has begun than to prevent it in the first place.

Keeping Your Devices Clean

An important part of digital hygiene is keeping your computer and other devices "clean." That means avoiding spyware and other malware (such as viruses and other applications designed to harm your devices or data). (Staysafeonline.org coined the term "keeping a clean machine" to describe this.)

Spyware and malware can be installed on your device in several ways. The most common are by clicking on a link, sharing a flash drive or storage device, or downloading or accepting a digital file. Malware is designed to harm your device or data. Spyware is used to "spy" on you, your files and what you do with your device. Some spyware can even give others access to your device by remote control.

Luckily, it's easy to avoid spyware and malware if you are careful and think ahead. Most good security program offered by well-known security software providers will help spot and remove most spyware, keep others out of your devices and files and prescreen for malware. Just make sure they are correctly configured and set to update automatically to keep you and your devices protected. Most work you're your computer, but some also protect your mobile devices from spyware and viruses.

Just as important as keeping a clean machine is locking your devices, accounts and files. This involves the use of the right passwords and selecting the right privacy and security settings.

Password theft or abuse are often the root of digital problem. They are easy to guess, hard to remember, stored on a device or shared with others. WiredSafety.org's studies have shown that most teens share their password with at least one other person (typically their boyfriend/girlfriend or best friend) and often adults do too. And we rarely use different passwords for different sites or purposes, which means once someone has it for one network, they have it for all networks.

Remember that giving your password out is like locking your door, but giving someone the key and burglar alarm code. It's not very smart. Make it a hard and fast rule never to share their passwords.

Too many computer and account intrusions arise just because the password was easy to guess (such as the word "password," or "12345") or because it was one of the "20 questions" used to come up with most passwords (such as our pet's name, our middle name, the street we live on, birthdate or anniversary, the year we graduated or will graduate high school, favorite sports team or rock star).

Use passwords to lock your devices when not in use, as well, and to protect certain sensitive files, folders and features. And, on Facebook, consider authenticating your device, by letting Facebook know which devices you use. This prevents your account from being accessed by someone else from a different device. It's a fast and easy way to avoid major problems.

We should also learn about privacy and access choices available for our favorite networks. We can restrict certain specific people or, in some cases, everyone except our friends from contacting us or being able to view our posts. Once we make their choices, we can enforce them using privacy, security and personal settings provided by the device manufacturer, service provider or network. You can read more on Digital Hygiene at WiredSafety.org and access materials and resources from the StopCyberbullying Toolkit at Stopcyberbullying.org.

ThinkB4uClick

We send tons of IMs and texts at the same time we are talking to friends in real life. It's understandable that we will end up sending a message to the wrong person by accident, or leave out words or emoticons (like smileys or frownies) that let them know what we really meant. A misunderstood message or a message in the wrong hands can lead to a cyber world war three.

Try and slow down long enough to reread what you are planning to send. Did you send it to the right person? Did you leave out an important word that changes the meaning? Will they understand what you meant? If not, take a second longer and make it right. Think about the person on the other side. Is what you are sending hurtful or sarcastic? Do they understand enough about the context of the message to understand it? Should you be using a different medium for the message? Some messages are better delivered in person (like breaking up), others can be done better by phone (complicated discussions) and some are just fine in texts and IMs (quick updates, sending a phone number, address or schedule). Some are public, some are more private. You should decide which is better in each case. The StopCyberbullying Toolkit has resources on selecting "the right medium for the message" and is available without charge to schools at StopCyberbullying.org.

Acting Fast

If you and your romantic partner break up, before you cry yourself to sleep or check the dating ads, change your password. If you get into a fight with your best friend turned enemy, change your password. Make sure you choose one that is easy to remember but hard to guess. The faster you act to lock out others from your accounts and groups, the better.

If you see cyberbullying, report it right away. Many huge cyberbullying campaigns could have been avoided if Facebook and other social networks knew about it early enough. The longer you wait, the faster it grows. Received a "sext"? Delete it. Do not pass it along, copy it, save it or print it. Get rid of it as fast as you can. Possession of child pornography is a serious crime. If the pic is of someone under the age of 18, in the US you can be charged as a sex offender for just having copies of these images on their device or online storage accounts. If you took a sext image, think before saving it or sharing it. The faster you engage your brain cells the safer you'll be. Delete it from your phone and destroy all digital or printed copies. Someone can easily grab your phone when you're not looking and broadcast it to everyone or send it to them to hurt you later.

Keeping an Eye Out

Facebook, Google, Bing and Yahoo! yourself. Search for your whole name (in quotes to search as a phrase). Search for your cell number, screen names and email addresses. Search for your nicknames and home address. Then set an "alert." Alerts send you a message any time the search engine finds this

information online. The faster you know about something that is posted about you that shouldn't be, the faster you can do something about it.

Some posts on social networks don't get picked up by search engines, so double checking there can help. Consider it an early warning system. While you're at it, keep any eye out to protect your friends and family members too. For more tips on keeping an eye out, read "Google Yourself!" on WiredSafety.org and at StopCyberbullying.org