Stalking & Technology

There are numerous new technologies that are being used for harassing and stalking. The tools perpetrators may use include:

- Social media pages like Facebook
- Hacking into victim's email accounts
- Installing Spyware on a victim's computer that monitors activity from a separate device
- Installing GPS devices or apps on/in the victim's car or phone
- Activating the victim's phone for tracking through the cell phone company

If you believe that someone may be using technology to harass, threaten or stalk you, document the activity and file a report with law enforcement. If you believe that someone is tracking you, stop using the device that may be compromised.

The Internet & Kids

Children are some of the most vulnerable internet users. It is important to remember that they may be more "tech-savvy" than prior generations, but they may not be aware of, or concerned about, all of the *risks* involved with new technology.

The internet also provides an arena for predators of all kinds to easily target children. If you have or know children who use the internet and internet capable devices (smart phones, tablets, music players, etc.) talk to them about internet safety and ensure that appropriate security settings are in place to protect them. For example, set up parental controls to block certain types of websites or to deny certain downloads.

Most importantly, talk to them about internet "stranger danger" so that they understand the risks and your expectations.

Who can help?

The Victim Advocate within the Laramie County Sheriff's Office can provide assistance with information about your case status, Crime Victims' Rights, Crime Victim Compensation, navigation of the criminal justice system and referrals to appropriate helping professionals or organizations according to your specific needs.

Resources

Federal Trade Commission Internet Safety website:
www.ftc.gov/bcp/menus/consumer/tech/privacy.shtm

WiredSafety is a US charity operating through volunteers. It is the largest and oldest online safety, education, and help group in the world.
www.WiredSafety.org

National Center for Missing and Exploited Children
www.netsmartz.org/

November 2013

Safety with Technology

Laramie County Sheriff's Office
Danny L .Glick Sheriff
307-633-4700

Name/ID Number:

Direct Number:

Mailing Address:
1910 Pioneer Avenue
Cheyenne, WY 82001

Technology and Risk

There is no doubt that modern technology is amazing. It allows us constant entertainment, to accomplish tasks we never thought possible, and to stay "connected" at all times. However, all this connectedness has a down side: safety risks. Modern technology leaves us vulnerable to the risk of everything from identity theft to stalking. Often, these crimes affect those who did not realize their information was at risk.

Basic Web Browsing

Rule #1: Secure Browsing and 2 Step Verification. When you access websites that contains or obtains any of your personal data, you should ensure that the prefix to the web address is "HTTPS" instead of "HTTP." This encrypts the page and protects against hackers accessing what's on it. Under your account security/privacy settings, you can (and should) choose this option for your Facebook and email accounts. You can also sometimes choose to be notified whenever a new device logs into your account. If a device you don't recognize logs into your account, change your password immediately and check for a breach.

Rule #2: If you're not SURE where it came from, don't click on it, open it or download it. Hackers and scammers will send you emails and post eye-catching links on web pages that can infect your email and computer with viruses, steal your personal information, or rope you into a scam. If you receive a suspicious email or one from an unrecognized email address, label it as "spam" and delete it without opening. If you are browsing and see a link that you are not positive is from a trusted source, just avoid it.

Rule #3: Perform routine computer security checks and maintenance. Purchase a computer security program to scan and clean your computer of viruses, spyware and malware on a daily or weekly basis. Contact your local computer store for suggestions or read online reviews. Also, regularly delete your browsing history, clear your "cache" and delete your cookies (cookies store information about your web activity). You can find the options to do all of these things in your internet settings.

Facebook and other Social Media

Rule #1: Be Careful What You Post and Who You "Friend" Or Exchange Messages With. Do not divulge personal information on your status updates or posts to others' walls. Some examples: Do not leave your phone number or address on anyone's wall. If you are linked to anyone you don't want knowing your whereabouts - don't post your location. Do not talk about personal or legal issues, details about your job, etc. *Do not get involved in posting arguments.*

There is no reason to be friends with everyone who wants to be your friend on Facebook, especially strangers or people you have conflict with. Ignore requests and messages from people you are not SURE you can trust, and periodically go through your list to delete people you don't talk to anymore. The same for messages – delete without opening anything that is from someone you don't know well.

Rule #2: Make your account private! For safety planning above and beyond identity protection, it is best to choose the most restrictive/secure settings in each setting on your account and profile. For example, ensure that only your friends or a custom list of friends can see everything on your profile, including posts, pictures and other activity.

Rule #3: Beware of strangers! It is especially important to be cautious when meeting someone online to make a friend, for dating, or a one-time transaction (like a sale). Do not give personal data to someone you recently met online. If that person is coming to your home to buy something from you, make sure you are not home alone. If you are going on a first date, meet at a public place like a restaurant. If you get a bad feeling at any point in time - get out of there!

Rule #4: Beware of Enemies! If you have an ex-partner (or anyone in your personal life) who has become harassing or threatening to you for any reason, limit or cut off your online relationship with that person. Ensure they do not have access to your whereabouts through your account or your friends' accounts. If they are harassing or threatening you through Facebook or other technology, document all of the incidents and contact law enforcement.

Generally: Do not talk about personal matters that could allow a stranger or a dangerous person to know more about you than you would like. If in doubt, ask yourself if you would want a dangerous person to know what your wrote. If the answer is no, don't post or share it.

Helpful Hint: Employers are looking at Facebook activity too! If you don't want your boss to see that *one* picture of you...don't share it!

Your Personal Information

Passwords: Keep your passwords private, and make sure they are complex. Try to always use a combination of upper and lower case letters, numbers and symbols. Try not to use any real words in your passwords—use acronyms instead. Change your passwords regularly, and do not use the same one for everything.

Do not store documents with personal information in your email or in unsecured folders on your computer. For example, do not keep documents with your Social Security, bank account or credit card numbers where a hacker could get to them. If you provide this information over the internet, for example for a transaction, ensure that the website you are using is reputable, starts with "HTTPS" and does not save your logon information.

REMEMBER: The internet is forever. Nothing that is deleted on the internet is every truly deleted. And it's usually the bad guy that finds it.