c-hq security services
Technical Consulting

Focus on cyber-stalking

Cyber stalking and cyber bullying are a similar crime in that the same techniques are used to intimidate a victim. Cyber bullying might be considered a lesser crime by the inference within the name. However, whatever label it has cyber-crime is still a crime.

This article sets out to discuss some of the more basic issues related to cyber stalking and bullying. It differentiates these crimes from corporate or government cybercrime in that this article is intended to help individuals.

Cyber-crime has many challenges to overcome in order to prevent it or apprehend perpetrators. With the ever changing landscape of social media and advances in computing technology, the cyber-criminal adapts to find new ways to intimidate. It is important to remember that to protect ourselves, we must adapt as well.

METHODS OF INTIMIDATION

Identity theft – With a few simple details such as name and address a criminal can impersonate you. Given a date of birth and a password, the cyber-criminal can wreak havoc by setting up online shopping accounts, interfere with online banking and hack in to social media accounts.

Data Attack – An unprotected computer and network provides a criminal with access to your data such as personal photos, letters, hobbies and interests. The data can be manipulated or destroyed or even read and used against a victim.

Scare tactics – A cyber-stalker hides behind the internet and to many this means that they are elusive and untouchable. By issuing threats and manipulating personal accounts, the bully seams powerful.

False accusation – A cyber-stalker may make false accusation via social media or free access web sites to try and incite others to abuse the victim. Adult content sites and accusations of paedophilic activity are common techniques for damaging the reputation of a victim.

There are many other known techniques that a cyber-stalker may employ from false victimisation to GPS tracking. E-bombs will swamp your inbox with junk e-mail and micro cameras can record your activity. The YouTube Nation means that getting information broadcast is relatively easy.

HOW THEY TRACK YOU

The methods of information gathering employed by cyber-criminals are broad ranging. There are many free access websites that already post personal information about you for anybody to see. People tracing sites list your last registered address along with the people that lived with you at the time. These sites also track your social media activity and any information that you may have posted such as photographs and blogs. Other websites such as property sites will declare when you bought your house and how much you paid for it. The cyber-criminal treats information like a jigsaw. The more pieces they have the bigger and clearer the picture becomes.

Phishing, key logging and spyware are all software applications that once installed on your computer can create a constant stream of your personal information to the outside world. These applications can be implanted by a seemingly innocent but rogue e-mail.

The cyber-criminal is not guaranteed to stay online. The area between cyber-stalker and stalker is grey. More serious accounts involve close contact tactics such as card skimming, GPS tracking and filming to gain information and intimidate their victims.

c-hq security services
Technical Consulting

Focus on cyber-stalking

PROTECTING YOURSELF

Protection against the cyber-criminal is a difficult subject to address because of shifting technology on the internet. There are three basic avenues of protection. The first is doing what you can to defend yourself from cyber intrusion. Secondly, if you are being stalked there are additional measures that you can take. The third is information gathering. If you are being bullied or stalked then proving the crime is often quite difficult.

VIGILANCE

- Password protect all of your accounts - use complex passwords
- Don’t use the same password for all accounts
- Install anti-virus and anti-spyware software
- Keep security software regularly updated
- Use advanced security settings
- Remember, if it’s on the internet and free it’s because you are the product
- Don’t carry security details in your wallet
- Be suspicious of unsolicited contact
- Be suspicious of unusual contact or content
- Never give out detail unless you are absolutely sure of integrity
- Regularly reset your passwords and PIN numbers
- Monitor your account activity
- Reset passwords if used on an unknown computer
- Be cautious of using geo-location services on your mobile phone
- Keep work and family activity separate
- Use encryption software to store data
- If you are suspicious, act quickly

SHUT THE GATES

- Reset all passwords and PIN numbers
- Check security software settings
- Create new e-mail and social media accounts
- Minimise use of cordless phones, baby monitors etc.
- Replace your mobile phone
- Review encryption software
- Regularly check your credit rating
- Regularly search your name on the internet

EVIDENCE GATHERING

It is critical to record times, dates and events by keeping a diary but to help the criminal investigation it is important to gather primary evidence. This is evidence gathered as close as possible to the source. There are electronic devices that can connect to your computer that record the time and date along with everything that happens on screen and everything that you enter on the keyboard. Software applications can indicate sources of malicious data through such techniques as e-mail and IP address tracing.

CONCLUSION

Protection is necessary to defend yourself from cyber-crime. Simple, user friendly tools and vigilance will go a long way to keeping you safe. If you are suspicious of a crime being committed then act quickly to alert the authorities, increase your defences and seek professional advice. Information gathering is key to resolving the issue. A crime without evidence is difficult to stop.

ABOUT C-HQ

c-hq provides effective technical advice based on the understanding of your threats, the associated hazards and their potential. We provide advice and guidance for the security of people and property, critical national infrastructure and the high security estate.

CARDHOLDER'S REPORT
OF STOLEN CREDIT CARD
eby authorized to take all steps
gal use of the above-nu