SPYING MOBILE PHONES ONLINE COOKIE KEY LOGGING DATA

INTERVENTION IDENTITY THEFT

PHISHING PSYCHOLOGICAL ABUSE

CYBERSTALKING

PHARMING COMPUTER INTERNET CONTACT

TROLLING ACCOUNT TAKE OVERS DIGITAL STALKING

HACKING INTO ACCOUNTS DIGITAL FOOTPRINT SOCIAL

CYBER AND DIGITAL SAFETY:

ARE YOU A VICTIM OF CYBERSTALKING?

paladin

National Stalking Advocacy Service

0207 840 8960

www.paladinservice.co.uk

Trust for London
Tackling poverty and inequality

BIG LOTTERY FUND

CITY LONDON

KGA

Esmée Fairbairn Foundation

Police Mutual Foundation

What is Cyber and Digital Stalking?

- Cyber and digital stalking is using the Internet, email or other electronic communications to stalk someone. They may occur as part of a wider stalking campaign or may be conducted entirely electronically.

- It can also be a prelude to physical violence and as a result all matters should be taken seriously when reporting to the police.

- We live in the digital age and therefore a lot of information about us can be found online.

- Cyberstalkers can be anywhere in the country or the world.

Is it a crime?

- There is no legal definition of cyberstalking but it is recognised as being different from harassment as it involves fixated and obsessive behaviour. This maybe to gather information, monitor or discredit the victim.

- Under the Protection from Harassment Act (PHA) 1997, amended by Protection of Freedoms Act 2012 and two new offences of stalking were introduced on November 25 2012.

- Section 2a prohibits a person from pursuing a course of conduct that amounts to stalking.

- Section 4a prohibits a course of conduct which amounts to stalking involving fear of violence or serious alarm or distress which has a substantial adverse effect on victim’s usual day-to-day activities which the perpetrator knows or ought to know amounts to stalking or fear of violence.

- A course of conduct is conduct that occurs on at least two occasions. Most stalkers should be arrested and charged under Section 4a.

Stalking Behaviours

There are a number of ways that a perpetrator may stalk or harass someone through the use of technology. This includes but is not limited to:

- Sending unwanted messages, whether this be via email or social media, which may be obscene or threatening in nature.
- Identity theft.
- E-mail hacking – either by attacking the mail server or attacking the sign-in page with password cracking software:
- Hacking software is also available on the internet as well as automated hacking websites.
- In some instances a victim will think they are being directed to the correct web page, but it has been falsified.
- This type of hacking may include an entire account take over or be used to monitor what that person's online activities are, i.e. who they're speaking to, what activities they are engaging in.
- Social media account takeovers, changing of passwords and information.
- Using social media including Twitter, Facebook, WhatsApp, Instagram, LinkedIn and YouTube etc. to monitor someone.
- Fake profiles being set up in an individuals name, posting malicious content.
- If a perpetrator has access to someone's device then they can down load software to that device and use it track or monitor them.
- Software can also be used to download data from that particular device whether it be a mobile phone, computer, tablet or laptop.
- Other applications can also be used to access someone's webcam.
- Using others to gather information or target the person - online communication can also make it much easier for a third party to become involved.

Protecting Yourself

You can never be completely safe online, but here is some advice to stay safer:

DO

- Choose a strong password for all of your online accounts such as your bank accounts, emails, social networking sites and other online accounts. Weak passwords make it easier for someone to access your online accounts. Make sure it is at least 15 characters long and uses alphabet, numeric, special characters & a mixture of upper and lower cases. Avoid using dictionary words, and instead you could use a passphrase, for example: “Il!k3ch0col@te5”.
- Make use of security question options – don’t feel that you have to provide relevant answers – for example, for maiden name use “penguin” this will then prevent those that know the true answers from accessing your accounts.
- Make sure that you have good anti-virus and anti-spyware software installed on your electronic devices that you use/own such as computers, laptops, tablets and smartphones.

DO NOT

- Save passwords if/when it asks you whether you want it saved to the computer
- Choose security questions and answers which the perpetrator may know the answers to.

Who Has Access to my Device?

DO

- Limit the information you share and beware of saving usernames and passwords.
- Ensure you have a PIN code activated on your phone and/or tablet if left unattended others cannot access it.
- Disconnect your devices from networks as it can restrict a perpetrator from tracking you online.

- Take your devices to a local specialist if you believe that your devices have been compromised and ask them to perform a manufacturer factory reset and check if any malware has been downloaded onto the device.

DO NOT

- Leave a computer unattended whilst you are logged in if you are in a public area.
- Open attachments in emails that you do not recognise: keystroke logging software can be used to record (or log) the keys struck on a keyboard, typically in a covert manner so that the person using the keyboard is unaware that their actions are being monitored. If attachments are opened a virus and then imbed itself into the device and can be very difficult to trace.

How Can I Limit Information About Me Online?

- Ensure that you are not disclosing your name, age, gender of yourself, family and friends on websites.
- Google yourself to check your digital footprint frequently. If websites are displaying information about you that you want removed, contact the website administrators directly or the host via (https://who.is/)
- Set up Google Alerts on the advanced settings so you can be informed if your name, e-mail address or postal address, or telephone number(s) appear anywhere online.
- Ensure you keep information you share online to a minimum.
- Consider the use of internet browsers that do not collect cookies such as Aviator : (https://www.whitehatsec.com/aviator/)
- Consider using a name that is not your real name when you create an email account. Use a nickname as your email name, screen name or user ID. Ensure you do not use your birthday as the digits in your email name or password. Instead, create a user name that is gender neutral.
- Set up a separate e-mail account so if you were to remove yourself at a later date, you can just stop using that email account.

- Remove yourself from 192.com (http://statics.192.com/rel-b417/downloads/C01.pdf)
- Remove yourself from the electoral register, contact your local council on how to do this.

DO NOT

- Disclose your birthdate, city, schools, work or clubs addresses and other additional information.
- Release any personal numbers, phone numbers, bank details or your National Insurance number.
- Say where you are going, on social media – post where you have been.

Do you know who you're sharing information with?

Social Networking

Social Networking Sites enable people to stay in touch with their friends, share experiences and photographs. However, living our lives online and disclosing too much information can put us at risk.

DO

- Familiarise yourself with and use privacy settings on social networks so that only you and people you choose are able to see your profile(s) and information you share on there. Privacy settings regularly change so ensure you are up to date with them.
- Use the privacy features to restrict strangers' access to your profile. Be guarded about who you let join your network.
- Make it clear that if messages are unwanted, then say so. Tell them if they are causing alarm and distress and if it continues you will report it to the police.

DO NOT

- Accept friend requests from people you do not know or are unsure about.

Online Dating

Many now people use online dating websites due to our busy lifestyles.

DO

- Consider your safety and who else may be using these sites.
- Check before you join that the site is a member of the Online Dating Association (www.onlinedatingassociation.org.uk)
- Choose a username without your surname in it and keep your contact details private.
- Take your time before connecting with someone online as well as meeting up offline.
- Your research on them.
- Report unacceptable behaviour.

DO NOT

- Share any intimate pictures.
- Respond to requests for money.

What to do if your accounts are compromised?

REPORT IT

- If your Facebook account has been compromised or your stalker is posting inappropriate material or messages you can submit a report to Facebook either by clicking on the post or clicking on the help menu.
- If you are experiencing stalking via Twitter, ensure you report to Twitter: (https://support.twitter.com/articles/15794-online-abuse)
- If you feel that your Twitter account has been compromised you can download your account data via looking at your Settings on your device. https://womenactionmedia.wufoo.com/forms/wam-twitter-harassment-reporting-tool/

Geo-tagging

- Geotagging is the process of adding location data to various media such as photographs and videos. The data will include the coordinates of where a photograph or video has been taken. Geotagging occurs on most smartphones and tablets.

DO

- It is important not to give apps permission to access your location data unless you fully understand the implications for doing so. Check your settings on your devices for each app you have downloaded. You can turn it on and off as and when required.
- Turn off the GPS facility on devices unless absolutely necessary and ensure that this is also done for social networking sites.
- Avoid uploading photos that would identify personal information i.e. taken outside your house or beside your car.
- Set privacy settings so any photos will require your permission before it is posted.
- Be aware of ‘Checking-in’ tools such as Facebook or Foursquare which enable users to share their current location. Know who can see your information. Use tools such as the Facebook Profile Review which means you will be notified when someone ‘tags’ you in a post.
- Be mindful of what your friends and family post about you online.

Safety for Children

Remember, it’s not just what you post

It’s also what your children post. Ensure you talk to your children about safety online and make sure they are aware of privacy settings on social networking sites. Talk about why they should be hesitant to accept friend requests form people they don’t recognise or who they aren’t familiar with.

Effective Evidence Collection

Ensure you proactively collect and keep the evidence:

DO

Keep a hard copy. Print evidence off and keep a record.
Take screenshots – this might be emails received, fake accounts set up. If possible keep them with someone you trust, don’t store them on your device where someone could gain access or delete them. Ensure that you collect any evidence from social networking sites and emails before removing them so you can show them to the police.

Also use the application ‘Paint’ to highlight areas of the evidence.

If you print off evidence, it is also helpful to ask someone to sign and date the documents to confirm that the email was received and they have seen it.

Keep voice recordings – if you are receiving phone calls or voicemails, set up the voice recording option on your phone in settings to capture what has been said. You can aim to track the location of call. By recording it, you will also have the time and date logged. Saving these for evidence collection:

- For iPhone: (http://www.tech-recipes.com/rx/6403/iphone-transfer-voice-memos-from-iphone-to-computer/)
- For Android: (http://www.wikihow.com/Record-Voice-With-Android)
- Use a Dictaphone to record if you don’t have a smartphone.

Time and Date Stamp - A time stamp is a term used to describe a time that is attached to a file or email to help keep track of when data is added, removed, sent and/or received. Similarly a date stamp is the date attached to a file or email.

Don’t Suffer in Silence – REPORT IT

6 GOLDEN RULES:

R eport it as early as possible to the police and tell others what is happening. Tell your family, friends, neighbours, workplace, children’s nursery and school.

E nsure you get good practical advice – Paladin or call the National Stalking Helpline 0808 802 0300.

P roactive evidence collection – keep all the evidence, including messages, emails.

O verview of what is happening – keep a diary – including time, date and details, available on Paladin website.

R isk Checklist – complete the S-DASH 11 screening questions http://paladinservice.co.uk/advice-for-victims/

T rust your instinct and never make contact with the stalker – If you are frightened or worried, call the police or go to a safe place.

Are you at risk?

Ask yourself these questions:

1. Are you very frightened?

2. Is there previous domestic abuse or stalking/harassment history?

3. Have they vandalised or destroyed your property?

4. Have they turned up unannounced more than three times a week?

5. Have they followed you or loitered near your home or workplace?

6. Have they made threats of physical or sexual violence?

7. Have they harassed or stalked any third party since the stalking began?

8. Have they acted violently towards anyone else during the stalking incident?

9. Have they engaged other people to help their activities?

10. Have they had problems in the past with drugs (prescription or other), alcohol or mental health?

11. Have they ever been in trouble with the police or do they have a criminal history?

If there are any positive responses, report it to the police. Call Paladin for further support and practical advice.

If you are in immediate danger call 999 and ask for the police

Jargon Buster for Cyber-Related Information

Antispyware Software
Software specifically designed to detect and prevent spyware.

Antivirus Software
Software specifically design to detect and prevent viruses on devices.

Central Processing Unit
The hardware within a computer that carries out the instructions of a computer program

IP address
Internet Protocol address – that connects you to the internet – to look for your computer/device you require your ‘IP address’

Keystroke logger
A virus or physical device that logs keystrokes to enable it to capture a users private information, passwords, credit cards information for example.

Log file
File that lists actions that have occurred on a device.

Malware
Software either used or created to interrupt the way in which a device operates. It is used to gather sensitive information or to gain access to private computer systems. Also referred to as malicious software.

Spyware
Malware that secretly monitors someone’s activity.

Date and Time Stamp
Character or encoded information used to recognise when a certain event took place.

Trolling
is when a person sows discord on the internet by starting arguments or upsetting people, by posting inflammatory, extraneous, or off-topic messages in an online community.

URL
Uniform Resource Locator - A ‘place’ on the internet, Facebook for example.

USEFUL LINKS & ADVICE

Police Practice Advice:
https://www.npia.police.uk/en/13968.htm

CPS Guidance:
https://www.cps.gov.uk.legal/s_to_u/stalking_and_harassment/

CPS Guidance on Cases Involving Social Media:
http://www.cps.gov.uk/legal/a_to_c/communications_sent_via_social_media/

Child Exploitation and Online Protection (CEOP)
https://www.ceop.police.uk/safety-centre/

Collyer Bristow - Cyber Investigation Unit
http://www.collyerbristow.com/personal/cyberstalking/cyber-investigation-unit

ThinkUKnow: https://www.thinkuknow.co.uk/

Get Safe Online – Free Online Security Advice:
https://www.getsafeonline.org/smartphones-tablets/viruses-and-spyware-st/

Introduction of Two New Specific Offences to Stalking http://paladinservice.co.uk/wp-content/uploads/2013/07/20121012stalkingcircular.pdf

Digital and Cyber Shorthand Guide
http://paladinservice.co.uk/wp-content/uploads/2014/11/Digital-and-Cyber-Stalking-Toolkit-2013.pdf

Safer Internet Centre http://www.saferinternet.org.uk/

If you require further advice contact:
Paladin National Stalking Advocacy Service
(T): 0207 8408960
(E): info@paladinservice.co.uk
(W): www.paladinservice.co.uk
(T): @paladinservice

paladin

National Stalking Advocacy Service

0207 840 8960

www.paladinservice.co.uk