Client Details: CARA Risk Level (if used):	Lead Support Worker:

Northamptonshire Police

Cyber Client Target Hardening Form for Domestic Abuse Partner Agencies

This form can be used by the client support worker to help in the creation of a Cyber Safety Plan.

If dealing with a HIGH risk victim of Cyber Stalking, then please contact Northamptonshire Police for further advice and support.

Speak to DC 789 Steve Watkins for further advice or support on completion etc

Northamptonshire Police

Helpful Online Information

Victim Details:	**Perpetrator Details:**

Known online sites the perpetrator is active (Facebook etc)	What public Wifi does the perpetrator use? (TheCloud etc)
What email addresses does the perp use?	Does the perp use Cloud Storeage (Dropbox, G-Drive etc?)
What mobile phone numbers does the perp use? (include provider, contract type and make / model of phone).	
What are the perpetrators Bank details ?	What passwords or PIN numbers does the perp use?
Details of any online criminality the perp is involved in	Details of drug / alcohol use by the perpetrator
Preferred method of perpetrator of accessing the internet	Any use of online Gambling sites? (details)
Details of the perpetrators Internet Service Provider	Details of online gaming (including gamertags etc)
Details of any Usernames and Social Media used by the perp	Any other specific information (MAC addresses etc)
Notes:	

Please submit this form via email to CyberCrimeUnit@northants.pnn.police.uk and include as much detail as possible please.

Explanatory Notes: Helpful Online Information

Known online sites the perpetrator is active (Facebook etc) This information helps to locate the suspect across social media so police can build up a profile of them	**What public Wifi does the perpetrator use? (TheCloud etc)** With the correct information , it may be possible to determine the location history and browsing habits of the suspect using the public wifi details
What email addresses does the perp use? Email addresses are used for many different reasons online and can help with location, accessing accounts etc.	**Does the perp use Cloud Storage (Dropbox, G-Drive etc?)** Details of online storage, particularly with passwords and usernames can help with determining online criminality.
What mobile phone numbers does the perp use? (include provider, contract type and make / model of phone). Mobile phone use can help to locate the suspect and provide communications data to determine harassment etc.	
What are the perpetrators Bank details ? Bank details allows police to conduct financial checks on the suspect, helping to locate them	**What passwords or PIN numbers does the perp use?** Passwords and PIN numbers are usually the same across platforms and can be useful, even if not used for every account
Details of any online criminality the perp is involved in Details of further offending can help with disrupting them.	**Details of perpetrators sexual preferences** Determining sexual preferences can assist with further intelligence development work in the future (Social Engineering)
Preferred method of perpetrator of accessing the internet This is useful to determine how to look out for the suspect online	**Any use of online Gambling sites? (details)** Determining gambling can assist with further intelligence development work in the future (Social Engineering)
Details of the perpetrators Internet Service Provider Required to conduct further communications data.	**Details of online gaming (including gamertags etc)** Can be used to find the suspect and determine online activity
Details of any Usernames and Social Media used by the perp This can help to find what platforms the perpetrator is active on	**Any other specific information (MAC addresses etc)** Any other useful information they can provide

Northamptonshire Police

Cyber Target Hardening

Objectives

STOP MONITORING—SECURE INFORMATION—REDUCE DATA LEAKAGE

(without isolating the victim)

Securing Your Mobile / Digital Devices

	Completed	Notes
Add up-to-date anti spyware onto every device		
Review all applications on all devices and check permissions to access services		
Deactivate WiFi and Location Services on all mobile devices		
Remember to consider all smart devices (thermostat, car, smart watch, Fitness pal etc)		
MEDIUM / HIGH RISK Do a Factory reset on all mobile devices		
MEDIUM / HIGH RISK Deactivate any Cloud Accounts		
HIGH RISK Consider replacing all mobile devices		
HIGH RISK Consider replacing the hard drive on a computer		

Remember to trust your professional judgement—If you think this is HIGH risk then mark it as such and contact Northamptonshire Police for advice and support on managing the risk to the victim

Explanatory Notes: Securing Your Mobile / Digital Devices

Detail	**Explanation**
Add up-to-date anti spyware onto every device	Ensure that a good anti spyware product is installed on every device. AVG offers a good free product (http://free.avg.com). This will help scan for current threats and protect against future threats.
Review all applications on all devices and check permissions to access services	On the mobile device, click "Settings" -> "Apps" or "App Manager" (depending on device) -> Select the app and then scroll to "Permissions". Check these apps to ensure you are happy with what they are accessing.
Deactivate WiFi and Location Services on all Mobile devices	Check that Wifi is disabled on all of the devices, and that Geolocation is taken off. Google search "deactivate location services on [name of device]". This should remain off unless there is a need for it to be activated.
Remember to consider all smart devices (thermostat, car, smart watch, Fitness pal etc)	Check all internet connected devices and ensure that the username and password is changed on each, that the permissions are checked and if necessary, consider removing them. This would include all smart devices—think about everything that could leak data.
MEDIUM / HIGH RISK Do a Factory reset on all mobile devices	Consider conducting a full reset of all devices. This will help to clear all online profiles from the devices, particularly if you are going to change your online services (such as having a new app store or google play store so the perp cannot see what you are doing).
MEDIUM / HIGH RISK Deactivate any Cloud Accounts	Remove all useful information and deactivate all cloud memory storage. Youcan create a new one immediately using a different email address and password. Consider, BT Cloud, Dropbox, Google Drive, iCloud, OneDrive etc)
HIGH RISK Consider replacing all mobile devices	If you believe that your device has spyware or tracking software installed, the safest option is to replace the device entirely.
HIGH RISK Consider replacing the hard drive on a computer	If you are worried about tracking software on a computer, then the safest option would be to have the hard drive replaced or to purchase a new computer.

Northamptonshire Police

Cyber Target Hardening

Objectives

STOP MONITORING—SECURE INFORMATION—REDUCE DATA LEAKAGE

(without isolating the victim)

Securing Your Online Accounts

	Completed	Notes
Consider using a password manager, or use a password code. As an example, take a website and use the vowels only (capitalising one letter and adding a punctuation mark) and add a PIN to it – e.g. Facebook, this would look like aEoo1454? This would produce a very strong password, easy to remember but difficult to crack https://howsecureismypassword.net/		
Change ALL passwords and PINs		
Change ALL online banking details		
Set up two step authentication on Facebook and consider changing profile		
Create a new, free email account using a main email client (such as Gmail, Outlook etc).		
Change every online account to back up or recover to this new email account		
Further Notes / Password Details		

Remember to trust your professional judgement—If you think this is HIGH risk then mark it as such and contact Northamptonshire Police for advice and support on managing the risk to the victim

Explanatory Notes: Securing Your Online Accounts

Detail	**Explanation**
Consider using a password manager, or use a password code. As an example, take a website and use the vowels only (capitalising one letter and adding a punctuation mark) and add a PIN to it – e.g. Facebook, this would look like aEoo1454? This would produce a very strong password, easy to remember but difficult to crack https://howsecureismypassword.net/	Having a fully secure password is vitally important. There are a number of free password managers which act as a 'vault' storing your passwords for you , with access via a secure master password. Ensure that any new passwords have no relevance to your life (i.e. no birthdays, pets names, children's names etc). A strong passwords might be, F20gErx£14LK*x This would be a good password as it contains upper and lower case, has no relevance to me, contains letters and numbers and has special characters (i.e. ?!””*etc) . Check the website opposite to check the passwords suitability).
Change ALL passwords and PINs	Every single password and PIN number for bank cards etc MUST be changed, even if you do not feel the perpetrator knows about the account. This ensures that all personal details are secure—ensure that the back up email address has changed (a google search for Privacy Settings or similar will show how you can do this for your particular account).
Change ALL online banking details	Consider changing your bank account, but at the least, change all usernames, passwords and passcodes. Ensure that the address is not the old address and restrict access to specific devices (again, a google search or a call to the bank can help with this).
Set up two step authentication on Facebook and consider changing profile	Ideally, you should remove your Facebook account, however at the very least you should remove all friends connected to him, ensure that your account is private, block his profile and do not accept friend requests without being certain of who the other person is. Never share personal or location based information on Facebook as friends accounts may be compromised without their knowledge.
Create a new, free email account using a main email client (such as Gmail, Outlook etc).	Creating a new email account which has no relation to you (e.g. bluetie452@outlook.com) and use this as your new main email account. It would also be worth creating a separate account for general use.
Change every online account to back up or recover to this new email account	Using your new back up email account, change your newly secured accounts etc to recover to . Check with google if you are unsure how to do this.

Northamptonshire Police

Cyber Target Hardening

Objectives

STOP MONITORING—SECURE INFORMATION—REDUCE DATA LEAKAGE

(without isolating the victim)

Increase Privacy / Update Tools

	Completed	Notes
Do a full internet search on name, then phone number, then for photos then on address to see if anything comes up.		
Remove excess information from all online profiles / accounts.		
Review social media and see which accounts need to be removed or 'frozen'		
Review friends list on social media accounts and remove non essential friends or associates.		
Update security and privacy settings across all accounts and platforms.		
Use different, new email addresses (don't just use one email account).		
Check for fake profiles, particularly dating sites and pornography sites.		
Add non tracker browser add ons to the internet browser		
Secure internet browsers (consider re installing and using a more secure browser such as Firefox)		
Consider using a VPN to help protect against Interception (HIGH RISK)		

Click onto this website for site specific advice about checking privacy settings

https://www.staysafeonline.org/data-privacy-day/check-your-privacy-settings

Explanatory Notes: Increase Privacy / Update Tools

Detail	Explanation
Do a full internet search on name, then phone number, then for photos then on address to see if anything comes up.	Try to find yourself on google, using your name, phone number and other personal details. If anything identifiable comes up, then take steps to remove it by contacting the company or securing the account.
Remove excess information from all online profiles / accounts.	Make a list of all your online accounts, then access each one and remove any personal or identifiable information from each.
Review social media and see which accounts need to be removed or 'frozen'	Check all social media and delete or freeze any accounts you do not use to prevent them being accessed.
Review friends list on social media accounts and remove non essential friends or associates.	Check your "friends" on every online account and remove any people you feel could be a risk to you or you do not know personally.
Update security and privacy settings across all accounts and platforms.	With the list of all online accounts, check all of the privacy settings and secure them to their maximum.
Use different, new email addresses (don't just use one email account).	Consider using different email accounts, where needed just to sign up to a site, consider a service like 10 minute mail (https://10minutemail.net) which provides you with a temporary email account which you can access using a web browser and expires after 10 mins. No sign up, and is totally free.
Check for fake profiles, particularly dating sites and pornography sites.	Check dating sites or porn sites if you believe the perpetrator will place you details on there.
Add non tracker browser add ons to the internet browser	Consider using a secure internet browser, such as Firefox (google firefox) and install anti tracking add ons, like "Ghostery". There are a large number of useful privacy add ons, free, in the store.
Secure internet browsers (consider re installing and using a more secure browser such as Firefox)	Where any internet browser is used, always use the privacy mode browsing to ensure records are not stored on the device.
Consider using a VPN to help protect against Interception (HIGH RISK)	Consider using a VPN like ZenMate which will freely change your location using the internet. Your DMI can advise further.

Digital Non Molestation Orders

Please detach for Family Law Solicitor to consider application for a Digital Non Molestation Order

(Part IV Family Law Act 1996 / Domestic Crime and Victims Act 2004)

Consider applying for a non molestation order with any of the below relevant non molestation orders:

- Delete all existing pictures of the named victim
- Do not publish or distribute any images of the victim
- Do not access [name of child] mobile phone
- Do not send [name of child] any electronic files
- Do not connect with [name of child] via social media where the victim is also a member
- Do not publish any information or comments about the victim online
- Do not use geolocation services to track the victim
- Do not use any tracking device to locate the victim.