BritishRedCross

Home Office

Refugee Women Digital Empowerment and Connect Project

Guide to accompany workshop 3

Digital Safety

This guide has been developed as a supporting tool for women taking part in the Digital Refugee Women Empowerment and connect project workshops. It is targeted at women who have refugee status, humanitarian protection or refugee family reunion and live in the UK. The project is funded by the Home Office Resettlement Asylum Support and Integration directorate.

We would like to thank the members of the VOICEs network and Voices Ambassadors who have supported the creation of these legacy documents. Materials are available in English, Amharic, Arabic, Farsi, Kurdish (Sorani) Somali, Tigrinya and Urdu. It is hoped that refugee women who were not able to take part in workshops may still find it of use to work through and explore the information here at their own pace.

Contents

Preface

This tool is unable to fully explore and explain all threats and measures of protection that are available to internet users but only hopes to draw your attention to some key points and where you can find further information.

We acknowledge that in discussing digital safety we touch on issues around Gender Based Violence, abuse and criminal offences, which can be sensitive and often taboo. Our humanitarian mission and the principle of do no harm means we are called to action to do what is in our power to tackle gender-based violence, including providing information to support people to make choices that empower them and decisions that protect them.

Throughout this guide you will find embedded links within the text, which if you click on these will take you to the website mentioned. For example, if you click here you will be taken to the British Red Cross website. Where possible, we have tried to include links to translated resources, but many of the links in this guide are for information which is in English. Whilst we acknowledge the limitations of automated translation, we have given information about how to use this function in guide two.
Comprehensive advice on digital safety including how to protect your devices, and steps to protect yourself and others from online threats is available from www.getsafeonline.org.uk, and the National Cyber Security Centre www.ncsc.gov.uk. More information and support for victims of online abuse are available from Stop Online Abuse – www.stoponlineabuse.org.uk**.** For more information or support to tackle or report any type of Gender Based Violence, domestic abuse or harassment contact Refuge or the National Domestic Abuse Helpline www.refuge.org.uk / www.nationaldvhelpline.org.uk 0808 2000 247.

If you have immediate concerns or want to report a crime, contact the Police – 999 (emergency) – 101 (non-emergency)

Key terms

Digital safety - practices and habits to keep yourself, others and your personal information safe when using the internet
Inter-personal - relating to the interactions between people
Online threat – a risk or problem that causes an undesirable event or action via the internet
Password - a secret series of characters which allows access to a computer system or service
Secure - remaining safe and unthreatened, not exposed to danger or harm.

What is Digital Safety?

Digital safety means being aware of and knowing how to protect yourself (and your data) from risks online. Often digital safety means just having a few good habits that make you less vulnerable to cyber-crime, fraud, or threats. This involves knowing some of the tricks that criminals can use to get people to part with them information or money, or to invade your private life.

The most common types of threat online are from

- Viruses and malware that try to steal ("hack") your personal information or account details, or install programs that can spy on you
- Online fraud where criminals try to convince you to hand over information
- Bullies, stalkers and abusers who take advantage of online anonymity to harass, abuse or control you.

Online threats have the potential to affect financial, emotional, and personal wellbeing. With this balance in mind, importantly, awareness of digital safety helps people increase their confidence online.

Essential digital safety recommendations

Having Strong Passwords

Email and all other accounts online are locked with a password, a key, to prevent others accessing your account. Making the password complex or "strong" is the best way to prevent someone getting into your private information.

Having a strong email password is essential. If a hacker gets into your email, they could reset all other account passwords by using the 'forgot password' feature and access sensitive personal information across all your accounts.

Hackers know many of us choose passwords like 123456, an important date in our lives or a child's name – do not be tempted to use anything that could be easily guessed. Easy passwords can be cracked quickly, but a good password locks out criminals. It is worth taking the time to invent one.

Follow these steps to create a new STRONG password:

1. join three random words: e.g., rug, fire, fork to make rugfirefork.
2. Add uppercase letters, e.g., RugFireForK
3. Add Numbers, e.g., 19RugFireForK90, and
4. Add symbols to make the password more complex: !19RugFireForK90!

Hackers share lists of millions of compromised passwords and three random words is an easier way to create new passwords that are more likely to be unique to you and less likely to be guessed. It is strongly advised that you change your passwords periodically and do not use the same password for all your accounts. A password generator is also a good choice if you struggle to invent new passwords.

Use a password manager

If you are worried you will not remember 'strong' passwords, you can use a password manager. Password managers can mean saving your password in the web browser (such as Google Chrome or Microsoft Edge), so that the browser remembers the password for you. They are safer than using bad or weak passwords but remember to protect them in case of losing your device. Some companies specialising in antivirus and online safety (will provide a password manager as standard if you buy their antivirus tools; other companies will offer password managers on their own.

Set up Two-factor authentication

Two-factor authentication adds another layer of protection to your account by asking for another piece of information in addition to your password. This helps stop others getting into your accounts, even if they have your password. Guidance on how to enable Two Factor authentication for popular email and social media can be found on the **National Cyber Security Centre** website here.

Protecting your devices from viruses

Viruses are hidden programs that are transmitted by websites, email links, attachments or removable media (like USB sticks). They can cause a lot of disruption and can lock you out of your computer or accounts, steal personal information or data to sell or use, take your money, or even watch you in your home. Worryingly, not everyone knows how to, or takes steps to protect their devices from these threats. The ONS reported that in 2020, of those adults who have a smartphone, 17% did not have security on their smartphone and 32% did not know if they had security or not.

Like a security guard, **anti-virus** is a tool installed on a laptop, tablet or phone that stops these problem-causing programs infecting your devices. Anti-Virus protection for a computer, laptop, tablet or smartphone is important to help prevent common threats like:

- **Trojans** which pretend to be a program that you want to download (like an antivirus programme, a photo or a free film) but are or contain malicious software (malware) that becomes active when you install it on a computer or phone.
- **Spyware** which tracks information and watches what you are doing on your PC for criminal purposes,
- **Adware** which opens pop-up windows that try to sell you things.
- **Ransomware** which locks you out of your device and demands payment.
- **Spam** generating programmes called worms, which go into your system through open web connections, and replicate to send lots of unwanted "spam" emails out to your contacts. Unwanted email communication is referred to as **spam** or **junk email**. Spam email can simply be a nuisance, but it can also be used to defraud people and to spread misinformation.

Most systems will have some **antivirus or spyware** protection already installed, for example laptops with Microsoft Windows10 will already have Windows Defender installed.

You can get extra antivirus protection: Sometimes this is free, but there are also companies that provide paid programs.

Older software may have holes that viruses can sneak through. **Updates** allow these holes to be patched. You can arrange for programs and software to update automatically to patch any holes in your security. This means you do not have to remember to do it. Sometimes you may have to update the device manually and will usually get a reminder if this is the case. Do not ignore them!

Back up your data

Viruses can delete or steal your data and information. To protect your personal photos, files and information you should back up data before updating your device. Back up means create a copy, which can by physical using a portable hard drive, but more usually is to another device or in “cloud” (online) storage. This is because sometimes updates can change files, but if you have backups of your data that you can quickly recover you cannot be blackmailed by ransomware attacks. You can turn on automatic backup which means you don’t have to remember to back up your data.

Further guidance on backing up your data can be found here
www.getsafeonline.org/protecting-your-computer/Backups

In summary

- Do Keep a separate password only for your email
- Do check your email password and other account passwords are strong
- Do check you know how to change your password and do this regularly
- Don’t use the same password for multiple accounts and consider using a password manager if you are concerned about forgetting passwords.
- Use Two Factor authentication
- Do check you have antivirus and that it is activated (and get some if you aren't sure
- Do use and update your antivirus – do a full system scan regularly and update your antivirus to protect against newly developed viruses or bugs
- Do be careful what you download – ad or spyware programs get on your computer by attaching themselves to things you download so check where you get your files.

What to do if things go wrong

If you have opened a link on your laptop or have followed instructions to install something but have doubts, open the antivirus software and run a full scan. Allow the antivirus to try and fix the infection and restore your device by following the advice it gives. If it cannot be fixed you may have to get expert help.

Your close friend contacts you and seems very upset. They opened a file in an email that they thought was a photo. It was actually a trojan horse that hid ransomware and now they are locked out of their computer. What would you do, and what would you tell them to do?

If you have been infected with ransomware, be aware that if you chose to pay the ransom it will fund criminal activity and there is no guarantee that you will be able to access your device; unhelpfully it may give the impression that you are willing to pay again in future and invite future attacks.

Common types of online threat

Fraud and Scams

A scam is way to trick someone out of money or into providing their personal details, so a criminal can steal from their account or steal their identity. It can involve using viruses to steal data from their computer or online account or getting someone to willingly hand over money by misleading them or tricking them.

A scam is often conducted through using fake emails (**phishing**), text message (**smishing**) or phone call (**vishing**). Emails or texts may have a link to a fake website which tempts you to enter personal information or acts as a corridor and allows viruses into your computer. Or the email may have an attachment containing a virus that steals banking details, personal information or photos.

Scams make you think you are being contacted by an organisation you recognise or sometimes someone that needs help. They are designed so that you feel pressured to act, often quickly, to "do" something – open a link, give details, click on an attachment. Don't believe it!

We do not have enough time to list all types of scam and fraud here. More information on types of scams criminals use, as well as advice on how to report fraud and cyber-crimes can be found here: www.actionfraud.police.uk

Phishing

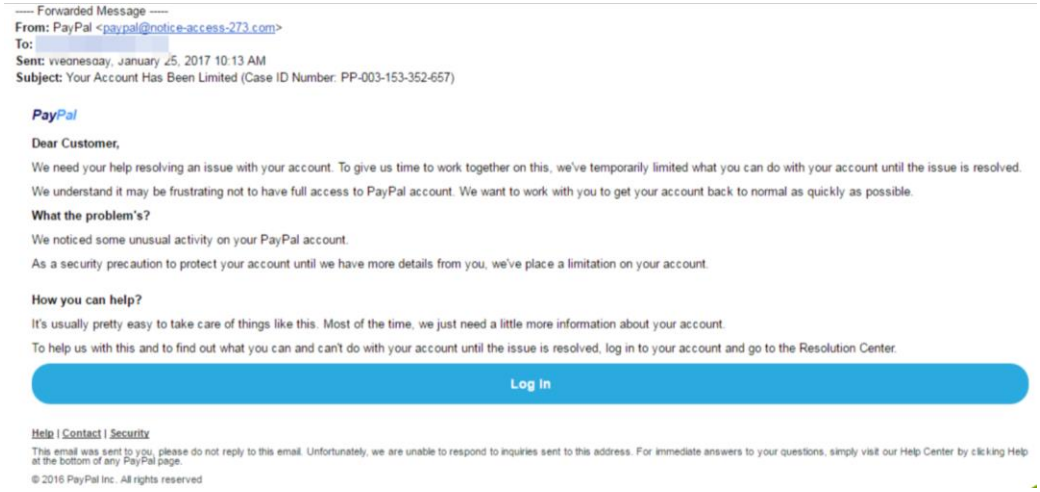
Phishing is a type of scam, where a cyber-criminal uses a "hook" to lure individuals into providing personal information, banking or bank card details, or account details and passwords. They then use this information to access your accounts and steal money or email contacts from you or to steal your identity. Criminals may send a phishing email to thousands of people hoping that they can trick just a few into giving them money or information.

Hackers and scammers will do an excellent job of pretending to be someone or an organisation that you trust, and they may even use your name and other personal information to try and convince you. They will try to lure you with an offer or bait you with a threat. For example, may pretend to be the government for example the tax office contacting you to offer a refund, but they need you to provide your bank details to pay you. They could pretend to be your local council, saying that you have a fine to pay or you will go to court, or pretend to be your bank or a banking intermediary like PayPal and that you are blocked from using your bank account.

Watch this video from the Metropolitan police on Phishing.

A quick way to check who really sent an email and whether it is a phishing scam is to look at the sender's email address, not just what shows up in "From". A real message will often come from a recognisable organisational address (e.g. noreply@yourbank.com) but scammers and criminals cannot use the real domain name of your bank or the organisation, so often the email address will be filled with random letters and numbers (e.g. noreply@1234bank12.com). If it is from a private address (e.g. person@gmail.com) it is unlikely to be from an official organisation – even Google do not use the GoogleMail (@gmail) domain to send organisational emails.

Looking at this example you can see that although it looks like a real email from PayPal, it is instead from a **different domain name**: Paypal@**notice-accessxxx.com**



---- Forwarded Message ----
From: PayPal <paypal@notice-access-273.com>
To:
Sent: Wednesday, January 25, 2017 10:13 AM
Subject: Your Account Has Been Limited (Case ID Number: PP-003-153-352-657)

PayPal

Dear Customer,

We need your help resolving an issue with your account. To give us time to work together on this, we've temporarily limited what you can do with your account until the issue is resolved.

We understand it may be frustrating not to have full access to PayPal account. We want to work with you to get your account back to normal as quickly as possible.

What the problem's?

We noticed some unusual activity on your PayPal account.

As a security precaution to protect your account until we have more details from you, we've place a limitation on your account.

How you can help?

It's usually pretty easy to take care of things like this. Most of the time, we just need a little more information about your account.

To help us with this and to find out what you can and can't do with your account until the issue is resolved, log in to your account and go to the Resolution Center.

Log In

Help | Contact | Security

This email was sent to you, please do not reply to this email. Unfortunately, we are unable to respond to inquiries sent to this address. For immediate answers to your questions, simply visit our Help Center by clicking Help at the bottom of any PayPal page.

© 2016 PayPal Inc. All rights reserved

It is worth being wary of emails that seem too good to be true, or that push you for quick decisions even if they use the right logos and look legitimate. Stay calm and question what you have received. Don't respond or click on any links. Once you open the link viruses may be installed on your computer to steal information, or you may be redirected to a malicious or fake website and asked to enter account or bank details which will then be stolen from you.

Recognising phishing and scam emails

- Do you know the sender? Are they addressing you in a general greeting?
- Are there spelling mistakes or is it poorly written?
- Does it want to you do something or is there a sense of urgency or is it threating you?
- Open the email address that the message has been sent from. Does it have the right domain name?
- Is it unexpected or from a company you have no business with?
- If it directs you to a website is there no padlock sign on the website and no https:// at the beginning of the web address?

More tips on identifying phishing emails can be found here: www.ncsc.gov.uk

Zahra receives an email which she thinks is from her bank – she opens it to learn that they say they have temporarily suspended her account. In horror, Zahra discovers her bank has found unusual activity on her bank account and decided to shut it down to protect her. It says she can't use the bank account until she logs in and reactivates it and asks her to click on a link. Zahra knows she has rent to pay tomorrow, and she must access her account immediately, but she is suspicious.

Zahra calls you for advice: What do you tell her and how might you advise her?

The link may be dangerous. It could mean that hackers will try to install something onto her computer for criminal reasons, such as to steal information or hack into her email, bank or social media accounts. Or the link may take her to another website (a fake version of the bank) that asks her for her ID and password or other bank details. Once she gives this information to the website, she will have handed the scammers her bank account and money.

Your bank will not contact you by email, phone or text and ask for personal details. If you are ever uncertain if it is really your bank calling you, and not a vishing scam, end the call and search for their customer service number online. Wait for 5 minutes before calling back or use a different phone as scammers can hijack phone lines.

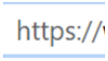
After talking to you:

Zahra looks online for the customer services telephone number of her bank. The bank confirms this is a fake email and her account is working perfectly. They tell her that the link in the email went to a website that was pretending to be the bank website. It can sometimes be difficult for victims of this type of fraud to get their money back if the bank can show that they were not careful.

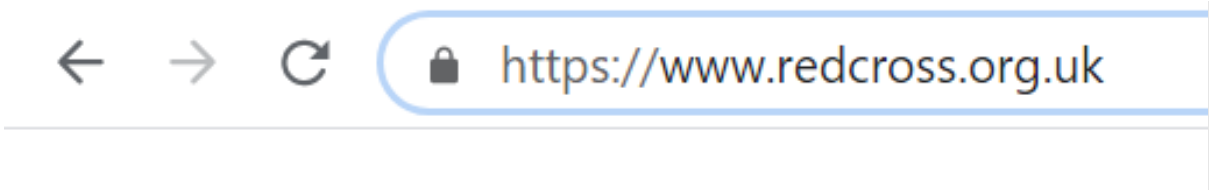
More information on phishing and scams can be found at the national cyber security centre. www.ncsc.gov.uk/guidance/phishing

Safe and unsafe websites

It important to be able to check whether any websites you visit are secure. Any website that you visit may prove unsecure, or hackers sending you fake emails may redirect you to a fake website which may look very genuine.

Look for this padlock logo  or these letters 

in the browser bar which means a website is secure.



Sometimes you'll see both a **padlock** and **https**, or only the padlock symbol, depending on the computer or browser. A website with only **http** may not be secure as the '**s**' indicates it is secure.

If you are asked to log in to an account, provide payment details or other information make sure any website you are using has "https" at the start of the address in the browser bar. Only enter log in details when you are sure it is the right website address and that it is secure.

Always type the full web address in to visit your bank's web page, espcially if you are logging into online banking. Never use a search engine to arrive at your bank's website, as this step can be used by hackers to compromise security and steal your details.

Take action against phishing and scam websites

To try to protect yourself remember the following tips:

- Keep your browser software, antivirus and spyware up to date
- Avoid risky websites that aren't secure or don't have a padlock
- Never click on a link in an email that is from an unknown or suspicious source
- Never give out your personal details, passwords or security codes over email or the phone

What to do if you have been targeted by a scam

Do Report the email, call, message or the website.

If you have received an email and you aren't sure about it, you can forward it to the **Suspicious Email Reporting Service (SERS)** at report@phishing.gov.uk. They will advise if it is or appears to be a phishing email.

If you receive a suspicious text message, you can send it for free to 7726. It allows your phone provider to investigate the text and take action if it is a scam.

Do not share your details but do check it out instead. Never call the number in the email or click on the links as they may direct you to another fake account. Go online and find the widely advertise number and call that instead.

Do not follow links without questioning where they are taking you. To check if a website is genuine, open your web browser and go directly by typing the name into the URL bar.

Never share your password or pin number. It doesn't matter if you think the person asking is your mother or best friend – do not give away your password.

If you have been tricked into providing your bank details tell your bank at once.

If you have lost money, tell your bank and report it as a crime to **Action Fraud** (for England, wales and Northern Ireland) or **Police Scotland** (for Scotland) By doing this you will be helping to prevent others become victims too.

Action Fraud www.actionfraud.police.uk

Relationships online

In this section we will talk about the impact of the internet in personal relationships. What we do online can directly affect our private life. Therefore, it is important to be very careful with the information you share with other people online.

We all want to connect with people, and it is one of the best things about the internet that we can easily communicate with friends, family and people with shared interests across the world. At the same time, it is important to understand that online connections need to be carefully managed, just as with meeting someone in the street, and that others may want to develop connections with people in bad faith that might lead to abuse.

Online abuse can be from complete strangers or people already known to you, and we will look at some examples of inter-personal abuse online below.

Romance fraud

Romance fraud is when someone uses an online dating website or app, developing an inter-personal relationship to gain trust and then ask for money or personal information. They will likely be using a fake profile to form a relationship, and they can seem genuine and caring. Quite often this person will ask lots of personal questions, but not show or tell too much about themselves. They will wait until they are confident that they have developed trust and use emotional attachment to ask for help, usually money, but it could also be to receive a parcel or supply an address. They may send false pictures or photos of themselves, which are often taken from elsewhere on the internet.

Never send or receive money or give your bank details to someone you meet online, no matter how much you trust them or believe their story.

It can be really upsetting or embarrassing to feel tricked into thinking you have formed a special friendship or relationship online, but you can report it to Action Fraud or call 0300 123 2040.

To check the source of an image you can do a *reverse image search* which as the name says, lets you search in the internet images to find others like them. You can do a reverse image check here

Cyber-bullying

Cyber bullying is a general term for bullying and harassment online or using technology. It covers any form of abuse online that is intended to cause another person harm, distress or personal loss. Often bullies use social media networking sites like Facebook or Twitter, messaging or interactive forums. Cyber bullying can be particularly distressing because via the internet and mobile phones it can reach people any time, rather than only in a specific situation such as school or work.

If someone has posted false or malicious things about you on the internet or on social media, it could be regarded as harassment which is a crime. Likewise, if you receive calls that threaten you or intimidate you the person making those could be committing a criminal offence.

Bullying can affect anyone, including both children and adults, but it is especially important to be aware of if you are a parent or carer of children. If you or your child or someone you know is being bullied, including online bullying, you can call the national bullying helpline for advice on 0300 323 0169.

Grooming

Grooming is when someone builds a relationship trust and connection with a person so that they can exploit and control them. Online grooming of children and young people is of particular concern, where a minor can be groomed for the purposes of sexual abuse (online or in person), drug trafficking or for other purposes of exploitation.

Grooming can take place over a short or long time and groomers may also build a relationship with the child's family to make them seem trustworthy, authoritative and helpful. Anyone can be a groomer regardless of their race, gender, age or relationship to the child.

Grooming can take place online where a groomer may present themselves as a peer to a child and send photos or videos of other people which support this. They may play games, give advice, show understanding and buy gifts for the young person in order to cement their position as a trusted friend, or try to isolate the child from family or friends, use blackmail to try and shame a child in to action or inaction, or introduce the idea of "secrets" to control the child.

More information on grooming is available from the NSPCC website along with other resources on how to talk to children about abuse and online threats. www.nspcc.org.uk

If you suspect a child is at risk do not hesitate to tell the police. You can also contact the NSPCC for advice and support to report abuse online.

Sexting and revenge porn

Sexting is when a sexual message, photo or video is sent to another person. A person might send a picture of themselves or of another person. A **sext** could be to a friend, partner or someone else online, and may involve partial or complete nudity, posing in a sexually explicit way or talking about sexual acts.

Whilst a sexual message could be sent between two consenting parties, pictures can be quickly shared over the internet without consent of the subject. Once somebody else has a picture or video shared online, they can send it to anyone.

Revenge porn is when someone shows or publishes a **private sexual** photograph or film of a person to another person or people, without the subject's consent and with **the intention of causing them distress**.

Threatening someone with revealing their private information and photos is also blackmail and a criminal offence. More information on revenge porn is available here

Revenge Porn Helpline – 0845 6000 459

www.revengepornhelpline.org.uk/

It is never okay for someone to pressure another person into sending nude pictures.

It's important to remember that images sent, even using services like Snapchat, can still be screenshotted and saved. If you have sent a nude or sexual image and you're worried about what might happen you can act through these tips:

- Ask for the message to be deleted.
- Don't reply to threats.
- Talk to someone and ask for support. You could contact the Revenge Porn Helpline.
- **Report what has happened**. You can report abusive content the website where the images are published. Most social media platforms have a tool to report content. You should also report this type of harassment to the police: Call 101 if it is not an emergency.

It is important to be aware that sharing a nude image of **someone under 18** is child abuse and a criminal offence under the Sexual Offences Act 2003. An act such as passing on a 'sext' of someone under 18 may result in a police investigation.

If you are worried about images of children being shared or have other concerns about child protection online, you can report these to the Child Exploitation and Online Protection safety centre. www.ceop.police.uk

Cyber-stalking and monitoring

Stalking is a pattern of behaviour from another person which makes you fear that violence will be used against you or which causes you alarm or distress and has a serious impact on your usual day-to-day activities. When it takes place online it is called cyberstalking. It can be gathering information on you, impersonating you, sending unwanted or threatening messages, watching you or getting access to your online account and spreading misinformation about you. A stalker can be someone known to you or a stranger. Cyberstalking can have a serious impact on its victim and is a criminal offence.

National Stalking Helpline – 0808 802 0300

www.stalkinghelpline.org/faq/about-the-law/

If you have concerns that you are being stalked or watched by an abuser:

- Avoid engaging with a stalker, who often wants to talk to you and build a relationship. Never agree to meet them and do not confront them.
- Do take it seriously and report the activity to the police. You can call 101 to speak to the police directly but if you think there is an immediate threat dial 999.
- Do check your privacy settings, ensure that minimum information is available about you online, and turn off location tagging on your device.
- Do alert people around you. They may need to check what they are sharing about you and may need to check their privacy settings too.
- Do keep a record of what happens – you may want to screenshot calls, messages or social media posts, which means you have a copy of the evidence even if the perpetrator deletes their messages and posts later.

Domestic abuse, harassment and monitoring

An abuser can potentially misuse the features of an internet enabled device to watch, check-on and control a victim. This can include monitoring your communication with other people, tracking your location through your device, or checking your financial expenditure. When these behaviours are perpetrated by a partner, ex-partner, family member or carer they are all considered forms of domestic abuse under UK law.

If you are worried someone might be monitoring your mobile phone or any other device the National Domestic Abuse Helpline has a walk-through tool to help you to change settings to make it safer.

National Domestic Abuse Helpline (24 hour) 0808 220 0247

www.nationaldomesticviolencehelpline.org.uk

Do you agree with the following statements?

Online threats don't really matter because it isn't the 'real' world

No. Online abuse is serious, has serious impact on people's lives and should always be treated seriously by authorities. Stalking, monitoring, and harassment are all high-risk behaviours which are not your fault. You have the right to report it, seek advice and be supported to address it.

The crime of harassment means being threatened in real life with violence.

The law states that harassment is when someone behaves in a way which is intended to cause you distress or alarm and the behaviour happens on more than once occasion. It can be different types of behaviour on separate occasions or instances. For example, one message intended to distress you is not harassment. Two messages may be harassment, or a phone call followed by a threatening email may be harassment. Other activities that count as harassment may be if you are followed, your home or work watched, your property damaged, or if you are maliciously and falsely reported to the police when you have done nothing wrong.

Zahra has a cousin who she is very close to. Her cousin had been acting differently lately appearing upset, irritable, and nervously checked her phone all the time when they are together. Finally, Zahra's cousin tells her that her she has not been sleeping well and she is very distressed by threats made by her former husband, who she is separating from. He messages her regularly and sends emails to say that she is a terrible wife and mother, and has brought shame to both their families, and that she must return and live with him. Zahra's cousin is extremely distressed recounting this.

She explains further that her former husband has a naked picture of her, which they had taken together when their relationship was healthier. He has threatened to send the naked picture to her family if she does not return to him.

Is Zahra's cousin a victim of a crime?

Yes. Zahra's cousin is a victim of **harassment and coercive control**. These threats are made against Zahra's cousin in order to try and exert control over her. The law states that this offence is when a person behaves in a way which is intended to cause you distress or alarm. The behaviour must happen on more than one occasion.

As this behaviour is conducted by her former husband, this harassment is a form of **coercive control** (a type of **domestic abuse**). It is a criminal offence. She should report this to the police.

It is also a threat of revenge porn, sharing her private sexual images without consent, with the intention of causing distress or humiliation. The threat on its own does not constitute an offence, however If Zahra's former husband shared this picture online, via email or social media, including WhatsApp or other messaging services, this would become an offence.

Zahras husband also speaks about family honour and their separation bringing 'shame' on the family. So-called 'Honour' violence is a form of abuse and Zahra may want to get support from an organisation who specialise in working with victims of honour-based abuse and

threats. **Karma Nirvana** run a telephone helpline Monday to Friday 0800 5999 247 www.karmanirvana.org.uk

Summary

- Think before you post. Don't upload or share things without considering how you would feel if it got into the wrong hands. Once you post something you lose control of it, particularly if someone else screenshots it.
- Protect your identity and don't share everything on social media. Social media is fantastic to let friends and family stay in contact but think about whether you may be telling the world more about your life than you intended.
- Consider carefully who can see what you are sharing online, check that your privacy settings are set to a high level and think about who you are talking to.
- Be aware of the signs of scams and how to look for scam emails and websites
- Never out very personal information online such as your address, phone number, full name, and date of birth.
- Never give out your log in details and passwords.
- Never open unknown emails, files or attachments and be aware of phishing and scams