

# Refugee Women



## Digital Empowerment and Connect Project

Session 3 – Digital Safety



Home Office

The power of kindness

# Welcome!

## Today we will:

- Discuss essential digital safety steps and tips on internet safety
- Discuss how to recognise types of common online threat
- Discuss how to relate online safety steps to social media and real-life interpersonal relationships



# Ground Rules

- Confidential space
- Safe space
- Phones on silent
- Be respectful
- Non-judgemental
- Talk one at a time
- Keep Zoom on mute if not talking
- **Do ask if you need something to be repeated!**
- It is okay not to know



# Digital safety



What does  
it mean?

Why is it  
important?

# Having a strong password

- Make your passwords difficult, so that this cannot easily be guessed by other people:
- Change passwords regularly
- Don't use the same password for every account
- Set up security questions in case you forget your password
- To make a strong password, a suggestion is to choose three random words, put these together and add numbers, uppercase letters and symbols e.g. Cat!PotatoS0fa7



See Metropolitan Police (2017) #threerandomwords  
[https://www.youtube.com/watch?v=3aY\\_EPgi0VU](https://www.youtube.com/watch?v=3aY_EPgi0VU)



# Protecting your devices from viruses

- Computers, phones and other devices can get viruses which can cause a lot of damage.
- **Anti-virus software** is a computer program used to prevent, detect and remove viruses.
- If you received a device from the Refugee Women Digital Engagement project, your laptop is set-up up with Windows Defender Antivirus. But, it is your responsibility to ensure your laptop has ongoing software protection.
- Anti-virus software needs to be regularly **updated**.

# Common types of online threat

## Email Scams

- **Email or text message, often with a goal to convince you to click a link.**
- Once clicked, you may be sent to an insecure website which could download viruses onto your computer, or steal your passwords and personal information.
- May use language which creates pressure to 'take action' such as open a link, give details or click on an attachment.

## Phishing

- Messages that try to **trick you into providing sensitive information** like personal data;
- messages may look very real and convincing and often appear to come from a bank or another trusted source
- you may want you to re-enter a password, verify a birth date, or confirm a credit card number;
- once your personal details have been accessed, criminals use it to commit fraud crimes such as identity theft and bank fraud.

## Malicious Software – 'Malware'

- Software that's been made by someone to cause harm on devices.
- Sometimes collects information or data saved on your device, and passes it on.
- Also known as **ransomware, viruses, worms, trojan, horses, spyware, adware, scareware** and **crimeware**.

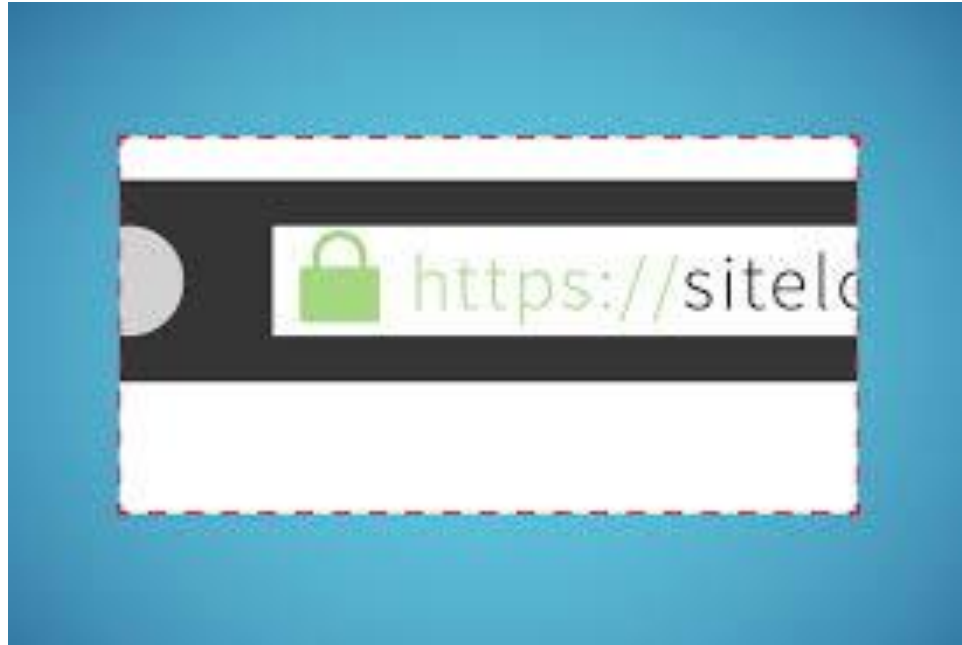
# Recognising phishing and scam emails

---

- 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 you to do something or is there a sense of urgency or is it threatening you?
- Does it seem too good to be true?
- 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?
- Does it re-direct you to another website?

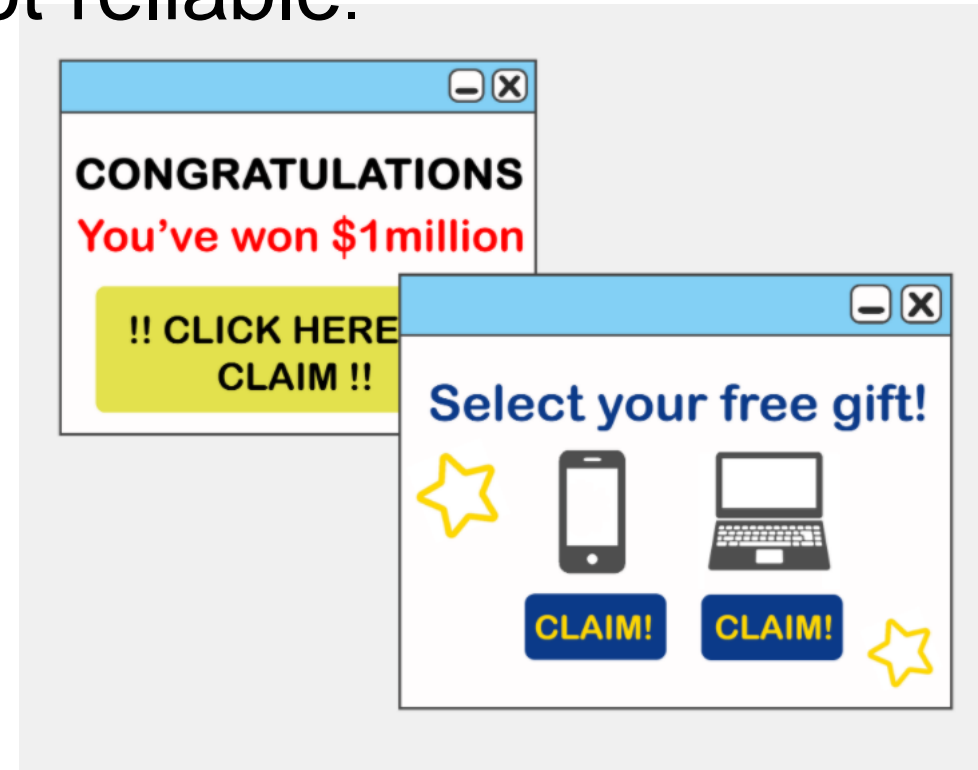


# Safe websites



Check for a **padlock symbol** and/or https to show whether a website is secure

'Pop-ups' on websites are often not reliable.



The power of kindness

# Safe searching

The image shows a browser window displaying the Google Search Settings page. The address bar shows 'https://www.google.com/'. The page title is 'Search Settings'. Under the 'SafeSearch Filters' section, there is a checkbox labeled 'Turn on SafeSearch' which is checked, and a link 'Learn more'. A dropdown menu is open on the right side of the page, listing options: 'Search settings' (highlighted with a dotted border), 'Advanced search', 'Your data in Search', 'Search history', 'Search help', and 'Send feedback'. The footer includes 'United Kingdom', 'Carbon neutral since 2007', and links for 'Privacy', 'Terms', and 'Settings'.

Search Settings

**Search results**

Languages

Help

**SafeSearch Filters**

Turning on SafeSearch helps hide explicit content, like pornography. SafeSearch preferences may be set by your device or network administrator. If you can't turn it off, check with the administrator of your network or device.

Turn on SafeSearch [Learn more](#)

- Search settings
- Advanced search
- Your data in Search
- Search history
- Search help
- Send feedback

United Kingdom

<https://www.google.com/preferences?hl=en-GB&fg=1> orks

Carbon neutral since 2007

[Privacy](#) [Terms](#) [Settings](#)

The power  
of kindness

# Clearing search history

The image shows a Chrome browser window with a 'New Tab' open. The address bar contains the Google logo. Below the address bar, there are several quick links: 'Apps', 'Sign in to your acco...', 'Online safety | Lear...', 'Managing your mo...', 'Improving your hea...', 'Help someone else...', and 'Home | Learn My V'. The main content area displays the Google logo and a search bar with the text 'Search Google or type a URL'. Below the search bar, there are several circular icons representing different websites: 'Worldwide H...', 'Voluntary Act...', 'Working...', 'The Guardian', and 'Migration Yor...'. A 'More tools' menu is open, showing options like 'Save page as...', 'Create shortcut...', 'Clear browsing data...', 'Extensions', 'Task manager', and 'Developer tools'. The 'Clear browsing data...' option is highlighted. A black arrow points from the top right corner of the browser window down to the 'More tools' menu. Another black arrow points from the search bar to the 'Clear browsing data...' option.

The power  
of kindness

# Connecting with people online



- Privacy settings for social media
- Social media content on search engines

### **Romance fraud**

- Development of an inter-personal relationship to gain trust and then ask for money or personal information.
- Uses the development of trust and emotional attachment to ask for help, usually money, but it could also be to receive a parcel or supply an address.

### **Grooming**

- Building of a relationship trust and connection with a person so that they can exploit and control them, often for purposes of sexual abuse.
- Online grooming of children and young people is a form of child abuse.

### **Cyber-stalking and monitoring**

- Stalking is a pattern of behavior from another person that causes fear or distress. When it is online it is known as cyber-stalking.
- Cyberstalking can have a serious impact on its victim and is a criminal offence

### **Cyber-bullying**

- Bullying which takes place online or using technology.
- Often bullies use social media networking sites like Facebook or Twitter, messaging or interactive forums.
- Can affect both adults and children.

### **Sexting and Revenge Porn**

- Sharing of private, sexual materials, either photos or videos, of another person, without their consent and with the purpose of causing embarrassment or distress.
- Sharing images of minors is child abuse.

### **Domestic abuse**

- Psychological, physical, emotional or financial abuse perpetrated by a partner, ex-partner, family member or carer.
- An abuser can potentially misuse the internet or internet enabled devices to watch, check-on and control a victim.

*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 previously in their relationship. He has threatened to send the naked picture to her family if she does not return to him.*

# Improving digital safety

---

What are digital devices?

---

What social media do you use?

---

What would be your advice?





**The power  
of kindness**



# Improving digital safety

Assess	Assess what online information exists about you like on Facebook and Twitter
Change	Change your e-mail and passwords for key online accounts
Delete	Delete existing online accounts especially if they contain large amounts of information or photos.
Review	Review all the privacy and security settings
Avoid	Avoid public forums
Limit	Limit what you share
Delete	You can delete your search history on Chrome, Firefox, Internet Explorer and Safari.
Set up	Set up a password or PIN for your computer or mobile device that ensures that only you can access it.
Email	Email: It is important to choose a password for your email that is unlikely to be guessed by another person.

# Summary

## Today we have:

- Discussed basic recommendations for digital safety
- Discussed some examples of common online threat and how to recognise these
- Discussed suggestions to check and improve your online privacy and digital safety.

**Importantly, digital safety is about awareness online.**



**The power  
of kindness**

# **Key words**

**Device** – electronic equipment which can connect to the internet

**Digital Awareness** – developing knowledge of the risks and benefits in using the internet and internet connected devices

**Digital safety** – practices and habits to keep yourself, others and your personal information safe when using the internet

**Online abuse** – cruel and damaging treatment of another person which takes place via the internet

**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

**Privacy settings** – controls which can be used to open or limit accessible information on social media.

**Social media** – websites and computer programs used by people to communicate and share information on the internet, using a computer or mobile phone.