Course notes: Helping others stay safe online

Congratulations on successfully completing this Digital Champions Network course!

These course notes are designed to be a summary of the key learning points and resources from the course and can also be used as a teaching aid. We hope you find them useful.

Key learning point #1: Understanding the fear

A recent survey of Digital Champions showed that almost half their learners were afraid to go online because they were worried about their privacy and security. These worries are real and understandable but also stop someone from benefitting from everything that the internet has to offer.

The risks associated with going online are similar to the risks we take in everyday life. You can make your learners aware of risks like hacks, phishing scams and viruses without being afraid of them.

Key learning point #2: How you can help

- Highlight the importance of anti-virus protection and firewalls and check that their internet connection is secure. Check out the guides on the course page for more information on how to do this.
- Help them use personal, shared and mobile devices safely.
- Encourage setting effective passwords and remind them to keep their passwords private.
- Guide them through using email and social media safely.
- Advise them how to keep their financial information safe.

Key learning point #3: Identity Theft

Identity theft can take different forms. It could be hackers getting someone's banking password and accessing their bank account. or it can be a criminal gang collecting enough personal information to open credit cards or apply for loans in someone else's name. But a few simple steps can help reduce the risk. There is more information in the Guides to identity theft and online safety available on the course page.

Key learning point #4: Device Safety: computer/laptop

Topic	Definition	Link
Anti-virus software	Prevents downloading a virus unintentionally. Anti-virus software needs to be kept up to date to provide the best	www.getsafeonline.org/personal/articles/viruses-and-spyware-2/

	protection, so it's worth checking your learner has auto-updates turned on.	
Firewall	A firewall is a barrier between your computer and others on the internet. Its purpose is to block attempts by malicious people to gain access to or destroy the information on your computer.	www.getsafeonline.org/personal/articles/firewalls/
Operating system	A computer's operating system (e.g. Windows or macOS) needs to be kept up to date.	https://protonvpn.com/blog/how-update-operating-system/
Internet connection	Make sure your learner is using a secured network.	www.safewise.com/online-security-faq/secure-internet-connection/
Shared computer	Remind your learner that it's ok to use a shared computer for example at the library, but they need to be extra careful about not saving passwords and not logging into online banking or making online payments as the network may be less secure.	www.safewise.com/online-security-faq/secure-internet-connection/

Key learning point #5: Mobile devices

- Ensure your learner has their device locked with a pin, thumb print or face recognition
- Help your learner to use the 'lost device' and 'find my device' functions (apple and android).
- Support your learner to understand how to know which apps are safe to use and which are reliable sources
- Talk your learner through how to safely dispose of old mobile devices
- Discuss safe and secure networks to connect to when out and about

The Get Safe Online website has lots more information about protecting your smartphone and tablet.

Key learning point #6: Passwords

- DON'T use anything personal or obvious (name, address, date of birth, pets), common or single words or the same password across all your online accounts.
- DO use sentences or phrases, the first letter of each word in a memorable sentence or phrase, numbers and special characters and at least eight characters – the longer it is, the harder it is to crack.

- Check out this short video on a great way to create (and remember!) a secure password.

Key learning point #7: Email safety

If receiving emails from an account you don't recognise you should

- Be cautious about opening these emails; put them in your spam folder so you don't get them again
- Don't open any attachments
- Don't click on any links or agree to download anything
- Don't respond to requests to enter log in details, passwords, bank or card details
- You should report the address to your email provider and delete the email. You can also report these emails to Action Fraud (www.actionfraud.police.uk/a-z-of-fraud/phishing).

Key learning point #8: Social Media

Quick tips to staying safe on social media include

- If you don't know someone, don't accept their friend request
- Make your account private or 'Friends only'
- Don't post pictures on public forums, especially of family members
- Never post your location, or refer to where people live or go to work/school
- Do not click on links if you don't trust them.

Key learning point #9: Online shopping

- Think before you click - if something seems too good to be true, it usually is! Advise your learner to beware of emails, texts or other promotions that encourage them to urgently click on links.
- DO your homework - fraudsters are fond of setting up fake shopping sites. Before buying anything, encourage your learner to read reviews and check trusted sources.
- Consider payment options - using a credit card has more protections than using a debit card. Alternatively, your learner could use a payment service like Google Pay or PayPal.
- Watch what you give away – Remind your learner to be aware of the kinds of information being collected when they pay for shopping online. Encourage them not to save their payment information in their profile.
- Use secure wifi – Avoid making purchases through public wifi. Show your learner how to use their phone as a hotspot instead.

Key learning point #10: Online banking

Here are some top tips to staying safe when banking online

- Don’t reuse the same passwords for different bank accounts.
- Use a strong password
- Never share your full password or PIN number - banks will never ask for your full PIN or password
- Always log out of your online banking session
- Be cautious when using a public computer to access your online banking
- Only use secure wifi networks to access your online banking
- Check your balance and transactions regularly, and report anything you don’t recognise to your bank
- Regularly check that your personal details are correct and up to date.