EDUCATION & TRAINING FOUNDATION

PROTECTING PERSONAL PRIVACY, DEVICES AND DATA ONLINE

SCENARIO 9

Original materials created on behalf of the Education and Training Foundation and funded by the Department for education

EDUCATION & TRAINING FOUNDATION

EDUCATION & TRAINING FOUNDATION

PROTECTING PERSONAL PRIVACY, DEVICES AND DATA ONLINE

Scenario 9

Refers to Modules

Protecting privacy

Protecting Devices and Data

Refers to Standards:

Protecting privacy

Protecting data

PROTECTING PERSONAL PRIVACY, DEVICES AND DATA ONLINE

Scenario 9

Using technology to manage personal, life and work relationships has brought immense benefits and changed the way people conduct their lives. It brings options for connecting people to talk, share, and trade what would be impossible by any other means.

It also improves efficiency in terms of time and effort to complete tasks.

Perhaps its greatest benefit is the potential in freeing-up time to spend on higher, more pleasurable pursuits and activities beyond the use even of technology itself.

Making this happen includes understanding what risks exist that might prevent this happening, through the potential actions of users themselves and others.

Understanding risks reduces their threat and increases the likelihood of technology improving all aspects of everyday life for all.

TEACHING TIP

This scenario explores how learners can best protect their devices, the data in it and data shared elsewhere in the Cloud, in order to find maximum pleasure and utility whilst containing risk of harm.

The critical learning point in the scenario is having users understand that their thoughts and actions are the best way of assuring this, and that technology can only go so far in achieving this. Relying on other people and systems only goes so far. A careless action or assumption is the biggest danger to things going wrong.

The aim of the scenario in discussing problems is not to frighten learners but help make checking second nature, allowing them to enjoy the huge benefits of web interactions with confidence.

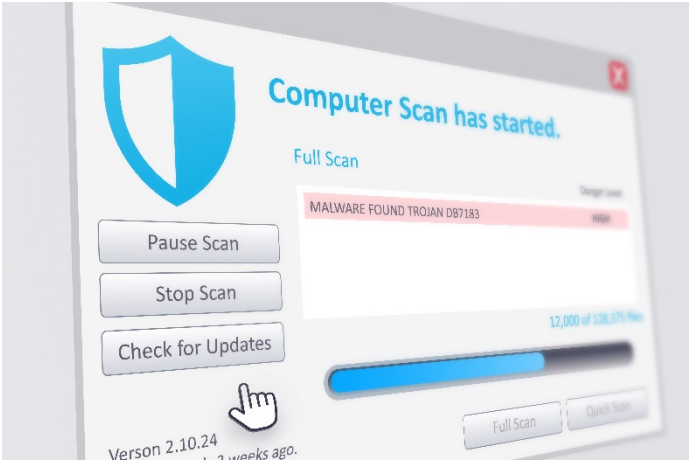
PROTECTING PERSONAL PRIVACY, DEVICES AND DATA ONLINE

Scenario 9

Why do we need protection?

The content held online by each of us has value. Others want to exploit that value in one of three ways:

1. By targeted advertising or sending out vast amounts of junk mail, using details of users' habits, customs, product preferences, etc.
2. By gaining access to valuable personal data, that is captured, taken or inadvertently, or shared with those able to exploit weaknesses in defence, and holding it hostage for a price or other motive.
3. Captured data can include financial records, academic accomplishments and other achievements and details that allow impersonation in transactions, using real accounts.
4. Claiming the ideas and accomplishments of others through copying and pasting thoughts, ideas, etc.



PROTECTING PERSONAL PRIVACY, DEVICES AND DATA ONLINE

Scenario 9

Most threats to privacy come about through either:

- The impersonation of a user that gives access to content, accounts and other sensitive material, achieved through hacking and overcoming technical defences.
- The unguarded reactions of users and how they respond to an approach. They share information in error, by deception or mistaken assumption.

The problem is, because technology is continually developing and moving forwards, many users are in a constant state of just about understanding how the technology works, then it changes!

It is a bit like a child being given a bike to ride, only to have it replaced by a bigger and better model, just before they fully master it.

It makes managing the risks trickier.

TEACHING TIP

Learners should understand that the vast majority of events where there is loss of privacy occurs at the hand of the owner who is tricked or fooled in some way to share of click a link that activates the fraud. (Entry level)

Keeping kit and content safe

It follows that users should take steps to prevent unwanted access to personal devices. This is true for work-related devices as well.

Watching out for viruses

Hidden, harmful software has to be added to a device to make it cause problems. Normally the owner innocently does this by opening an attachment or clicking on a link in a message.

TEACHING TIP

Work machines will have their own security protocols, but the issue of leaving a machine 'open' on a desk whilst away from it is a risk to data.

The rule really is, only click on a link you can trust. How you know you can trust a link is never certain, but common sense and 'if in doubt don't' is a good approach.

A judgement needs to be made about doing anything with an email that looks wrong.

Nuisance calls to smartphones can be easily dealt with. Disconnect and block the number (open the list of recent calls, click on the 'info' button against the call and 'block' is an option).

PROTECTING PERSONAL PRIVACY, DEVICES AND DATA ONLINE

Scenario 9

Accounts

An account is a set of personal data that is shared with an online service.

Logging into an account starts any new transaction from an advanced position because so much information is already set up, including presences in interaction.

The value of not having to repeat the upload of personal information, nor not being able to refer to the history of interaction, is immensely valuable.

TEACHING TIP

Ask learners to think what would happen if each time they wanted to use the library without an account.

- What information would need to be set up each time?
- How might items be reserved or renewed?
- Notifications sent against interests
- Reminders on loans
- How might the library and customer know who they were talking to and not at cross purposes?

The same discussion can be had on other online services.

PROTECTING PERSONAL PRIVACY, DEVICES AND DATA ONLINE

Scenario 9

Locking doors

Passwords are the best defence to access. Passwords are now capable of two-part authentication; users are able to use a message received on a second device that asks for confirmation to access the first.

This requires users to authorise their own access using a second device. This could be an iwatch, tablet, smartphone or laptop.

Another password that is increasingly used is fingerprint or facial recognition.

It is important that using relatively quick methods, device settings can 'lock' by themselves after a short period of inactivity. This is particularly important at work or study stations, where users may leave a desk unattended for a period of time.

TEACHING TIP

Discuss with learners how two-part authentication works and how it improves security.

Two pieces of advice for learners:

1. Use a mnemonic for remembering a password. For example:

   Oscar Wilde is reported to have said "I have nothing to declare except my genius" in 1882. Becomes 'Ihntdemg82'.

2. Don't use the same password for important accounts. Any potential problem is then confined to one account only.

Fraudsters

Fraudsters will start with the password 123456, because this is the most popular password in use. According to a CNN survey, it was used in 2019 by 23.2 million users worldwide.

If you were a fraudster and knew that 23.2 million users had 123456 as their password, where would you start? Adding a 9 on the end of the run is used by a further 7.7 million.

Use facial or fingerprint recognition and choose to use two-part authentication where possible.

https://edition.cnn.com/2019/04/22/uk/most-common-passwords-scli-gbr-intl/index.html

This is a good example of fraudsters relying on predictable behaviour in order to hack into an account or device.

It sits with other assumptions that an email that congratulates on winning a fortune or that an account has been hacked and needs repair, are also likely to catch attention.

Fortunately, major system providers offer password management apps. And they can be very helpful for major and sensitive accounts. Other apps are available too that are independent.

PROTECTING PERSONAL PRIVACY, DEVICES AND DATA ONLINE

Scenario 9

Rights to devices, data and personal reputation

Being safe starts with a clear understanding that all data and personal information is property that belongs to the owner. It can only be used by others in accordance with permission given (or withdrawn).

Like all property it has value (perhaps only sentimental) and needs proper protection.

Encryption

Encryption is using an algorithm to make data unreadable other than by the sender and the intended host.

It is used in financial transactions and other account-based activity. It can also be ‘turned on’ on personal devices to protect content generally.

Where available use encryption to protect data.

TEACHING TIP

In creating the right mindset, it is useful to have learners see content on devices as items of property, just as items are in their own home, with the ability to keep it hidden or share it, sell, or trade it with others.

No one would leave the front door open or store a piece of jewelry on the front wall.

If a caller asks you to share or check a fault on a bank account, hang up the phone, block the number, and check independently (if you feel the need). You don’t need the caller to help you check.

PROTECTING PERSONAL PRIVACY, DEVICES AND DATA ONLINE

Scenario 9

Learning activity:

Support learners in groups, or individually, to explore and share ideas on the following activities as part of a personal audit of online safety.

Physical protection of devices and content

There are two ways to keep devices and content safe.
Using settings on devices, find encryption options and consider using them to protect your content whilst it is travelling across the web and saved on devices.

Small is manageable

An advantage of portable devices means never being separated from small devices whilst away from home, and a good means of defence is the ability to not let a device be away from physical contact in public.

Keep portable devices in a pocket or particular place in a bag. Portability should mean always having them with you when out and about.

Where available make sure ‘Find my device’ options are turned on.

Copying to a separate plug-in hard drive

A useful method of protecting data is to provide a separate physical backup hard drive.

This is the equivalent of putting your money under the mattress, but this is a copy of precious files and the hard drive can be locked with a password.

Invite learners to look at buying a portable hard drive and what memory capacity they might want for precious files.

Leaving the door open and sharing too much

To be successful at impersonating users or accessing accounts, stealing content or devices, fraudsters are reliant on those they contact to make a mistake. That in turn is caused through an assumption, inattention, overly optimistic or concern of their victims that the fraudster exploits.

People gather in public spaces, shopping malls, large stores, coffee shops, and other public meeting places that often provide a public Wi-Fi for the convenience of customers whom they wish to attract.

Public Wi-Fi networks are not secure, meaning that a fraudster who gains access to the public router can see and capture content.

TEACHING TIP

Use 3G or 4G based devices in public places instead of public Wi-Fi.

Tethering a laptop or tablet through a smartphone, if available, is a good idea.

Keep interaction to a minimum, if there is no choice, and avoid using accounts if possible.

PROTECTING PERSONAL PRIVACY, DEVICES AND DATA ONLINE

Scenario 9

Finding a pseudonym

Teachers, police officer's, military, and many others change their name on social media accounts, in particular, to prevent them being found by someone completing a search.

Teachers would not want their school class asking to be friends on Facebook or Instagram.

Cautious mindset

Once users have a mindset about the value of their data, it should become second nature to only share what is required and not feel that adding information in some way makes the arrangement 'better' or improves the relationship, such as happens between people normally as they get to know each other better.

Users may choose to keep pictures and mementos that are never for sharing in any circumstances. But what if they are shared with someone where trust then subsequently breaks down. There is no 'back out' button.

TEACHING TIP

Don't offer or share information that is optional. Share what is needed to complete a transaction or as it suits a user's convenience.

Never post anything anywhere that you, or others (including future generations of your family) may regret or puts you at risk of exploitation at a later time.

Consider if you have and see if they can be deleted.

Check settings on personal accounts to make sure only essential sharing options are selected. Repeat for all apps and accounts.

PROTECTING PERSONAL PRIVACY, DEVICES AND DATA ONLINE

Scenario 9

Looking after data

There have been instances of government departments writing to individuals without hiding email addresses. This makes each of the addressees vulnerable to having their personal information misused by others in the same email. This information should be held in trust.

Deal with others' data as you would wish them to deal with yours. This relates to sharing, passing on, making assumptions about their likes, etc. without checking first and getting permission.

Explore address books and delete any contacts no longer needed.

Summary

Whilst it may not seem it, when thinking about the problems and risks of doing so much online, this scenario celebrates the fantastic opportunities of using devices across the web created for everyone.

Many web users want to talk to others who share their enthusiasm for the value of connecting and sharing and want others to assume the same level of commitment and honesty.

Sadly, not all do and those who don't will attempt to trade on the openness, honesty and willingness to share to exploit it for their own gain.

Extension activity

Using browsers to search the web leaves a trail or history. The value for users is that they can go back to required links, but the history can be collected by the browser owners and shared with others. It may lead to targeted advertising. However, the proliferation of cookies that can be stored from months' worth of browsing and opening websites, in addition to this tracking details, may make users want to think about their privacy.

Invite learners to explore their browser account and to think about how they feel about it in relation to user privacy.

Users may be pleased to have targeted advertising and location preferences enabled.

Using a browser accessed on a personal device, ask learners to count how many tracking cookies are in use (and consider whether to delete them). They are listed in the security tab of the browser settings.

Explore and consider using a new private window instead, as a means of keeping browsing private.

What are the merits or otherwise of using an AdBlock application? Ask learners to search adblocker in a browser for details.

Duckduckgo is a browser that does not to collect browsing information. How does this compare to other browsers such as Safari, Bing and Chrome?

(Level 1)

Further resources

Contract for the web.	https://contractfortheweb.org
A CNN report on the frequency of use of simple passwords.	https://www.cnn.com/2019/04/22/uk/most-common-passwords-scli-gbr-intl/index.html
Creative commons allows the attachment of attribution permissions to content that is owned, to show permission of how others can use it.	https://creativecommons.org
Guidance on how to spot a hoax email.	https://www.wikihow.com/Spot-an-Email-Hoax-or-Phishing-Scam
Find out about the regulations on Privacy and Electronic Communications Regulations (PECR). These explain the law with regards to marketing and advertising to email addresses.	https://ico.org.uk/for-organisations/guide-to-pecr/what-are-pecr/
Guidance from the Information Commissioner on all things relating to the management of personal data.	https://ico.org.uk/your-data-matters/
A detailed guide to two-factor authentication from Wikipedia.	https://en.wikipedia.org/wiki/Multi-factor_authentication
A guide from Symantec to two-factor authentication.	https://www.symantec.com/connect/blogs/guide-two-factor-authentication