

Online Safety

Workshop Outline
October 2026



Workshop Elements

A scaffolded approach to learning about online safety

- We will update our knowledge about
 - creating strong passwords and multi-factor authentication;
 - identifying and avoiding scams, phishing, and fraud; and
 - privacy protection and data management.

A review of curriculum resources and *OER that support a scaffolded approach to teaching online safety topics

- We will look at various learning resources and experiment with them.
- You will have an opportunity to experience some lessons as learners.

*OER = Open Education Resources



Why online safety?

Everyday internet use can include banking, shopping, messaging, schoolwork, social media, gaming, and cloud accounts. We all appreciate the convenience of being able to accomplish tasks and socialize online but every time we tap a screen or click a link, we might be leaving a piece of information about ourselves behind.

As we work, socialize, bank, and learn online, the boundary separating our physical reality from our internet existence has become blurred and it is hard to keep track of who has what information about us.

Online safety requires ongoing and active learning and is an essential life skill necessary to protect personal data, preserve financial and emotional well-being, and maintain the integrity of our digital devices.



Why online safety for literacy learners?

Literacy learners and their families, like all of us, are doing more and more online and it is challenging to stay up-to-date on possible dangers and proactive protections. Literacy learners looking to protect themselves and the people they care for may feel overwhelmed by all the possibilities and may feel insecure pursuing online learning and research opportunities.

Understanding the landscape and learning how to stay safe online will give people confidence to access digital and online resources.



Workshop 1: Learn together

What is online safety?

We will start with learning activities that

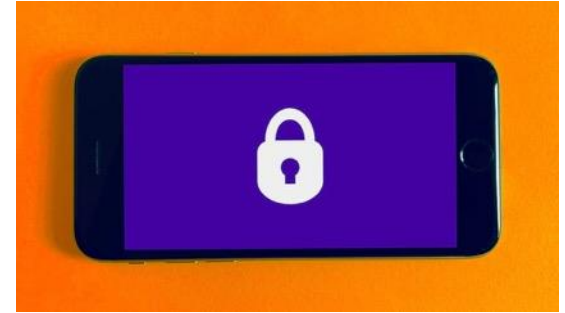
- introduce learners to the topic of online safety; and
- provide an overview of some of the places where we need to set up protections for ourselves.

Keeping accounts safe

Then we will look at some ways we can create good passwords and how to implement multi-factor authentication solutions.

We will

- explore lessons about the difference between passwords and passphrases, how to use password managers, and how to set up multi-factor authentication for our accounts; and
- test some tools for creating and testing passwords.

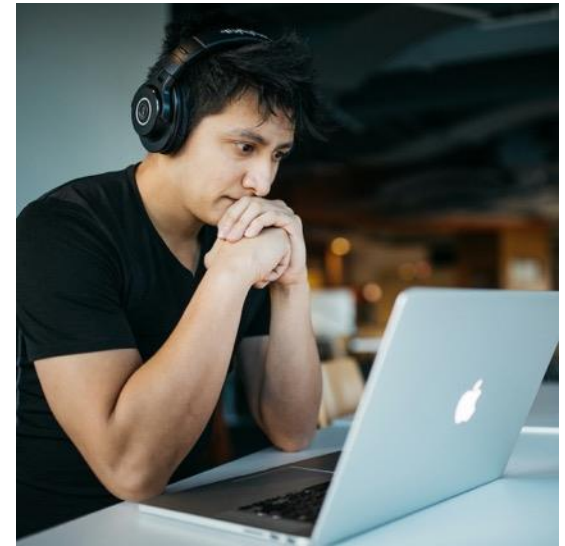


Workshop 2: Learn together

Identifying and avoiding scams, phishing, and fraud

We will

- explore lessons about identifying different online dangers (such as social engineering and phishing) and introduce learners to practices that can protect them from online scams and fraud; and
- review resources that provide tips safe web browsing habits and how to protect your device.



Workshop 3: Learn together

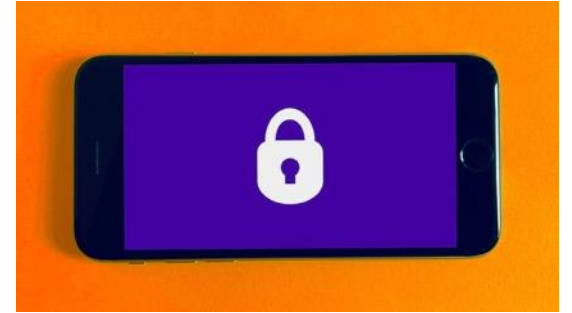
Privacy protection and data management

We are going to explore lessons and tip sheets that help us understand:

- what online privacy means;
- our rights and protections; and
- how we can protect our data and privacy.

We will provide you with an annotated list of resources for teaching possible online safety next steps:

- search engines and tracking;
- staying anonymous online;
- email and message encryption; and
- protecting ourselves on social media sites.



Knowledge developed in these lessons

I understand / recognize / am aware of

- Personal information has value and requires protection
- Awareness of common types of personal data (Personally Identifiable Information)
- How online activities can be tracked
- Data collection practices by companies and services
- Legal rights regarding personal data
- Not all online content and contacts are trustworthy
- Online threats exist (viruses, scams, hacking)
- Common cyber threats (malware, phishing)
- Basic security measures (passwords, updates)
- Secure password practices
- Software vulnerabilities and the importance of updates
- Reporting mechanisms and support resources



Skills developed in these lessons

I can

- Maintain security awareness in daily digital activities
- Create and remember strong, unique passwords
- Use password managers effectively
- Implement multi-factor authentication systems
- Identify what constitutes personal information
- Recognize privacy risks in online activities
- Verify the legitimacy of websites and communication
- Recognize suspicious links and attachments
- Identify and avoid basic scam attempts
- Recognize and avoid phishing attempts
- Configure device privacy and security settings
- Install and configure security software (antivirus, firewalls)
- Respond to security warnings and alerts
- Recognize when a device or account may be compromised
- Seek appropriate help for security issues
- Recover from common security incidents



Abilities developed in these lessons

I am able to

- Recognize when technical assistance is needed
- Follow basic digital safety instructions
- Adapt to new digital tools and platforms
- Maintain organized digital files and accounts
- Recognize when personal information is being requested unnecessarily
- Make informed decisions about sharing personal data
- Balance convenience with privacy protection

