



eSmart Libraries aims to build skills and behaviours for the smart, safe and responsible use of technology, contribute to digital inclusion and foster a greater sense of wellbeing for the library community.

What is it?





The eSmart Libraries program provides a framework for developing digital skills and cybersafety for library staff, members and the community of the Shire of Augusta Margaret River.

Why do it?

This is a great opportunity for library staff to increase their own digital literacy and awareness of cybersafety, and to be better equipped to help our community to be smart, safe and responsible online.

eSmart Libraries is a free framework to help you fully integrate cybersafety into your library

Why is it a good idea?

-  Builds on your library's existing cybersafety practices ✓
-  Helps you avoid cyber-risks and gain digital skills ✓
-  Provides you with resources and ongoing support ✓
-  Designed just for libraries and it's free to join! ✓

How did it start?

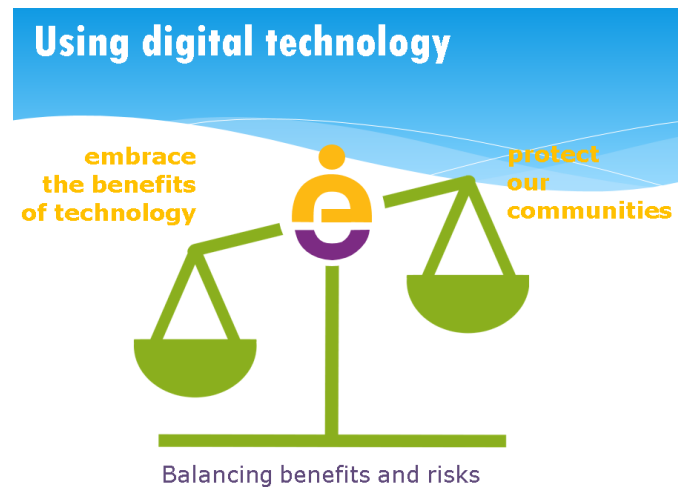
eSmart Libraries was initiated by a partnership between the Telstra Foundation and the Alannah and Madeline Foundation (a national charity protecting children from violence and bullying).

Library services who would like to gain eSmart accreditation follow a particular process developed by the eSmart national office. Although libraries may already be carrying out some aspects of eSmart, the tools and frameworks provided help busy libraries to follow this process in a methodical way. Many resources are shared so that libraries can benefit from documents already prepared by others.

An associated eSmart schools program is running in about 1,500 schools. eSmart is working with a similar number of libraries across Australia.

Components of eSmart ('Domains')

1. Vision, strategy and leadership
2. Library agreements and procedures
3. Staff knowledge and capabilities
4. Guidance and learning for Users
5. Community connections



Understanding cybersafety and cyber-risks

Cybersafety refers to the way in which people behave safely and responsibly to keep themselves and their friends safe online.

Cyber-risks include:

- Poor use of privacy settings on digital devices and social media
- Cyberbullying
- Malware
- Lack of password protection
- Scam emails and pop-ups

Scam emails

Easy ways to identify scam emails include:

- incorrect email for that institution/company, eg: apple@bzxy.net
- bad spelling or grammar
- email that claims that an account will be suspended if no action is taken

It's advised that staff sign up for the **Stay Smart** scam email alert service, a Federal Government initiative at <http://www.staysmartonline.gov.au/> This helps you to keep up to date on scams that borrowers might be receiving on email or by phone.

For a good overview of scams, visit:

http://www.staysmartonline.gov.au/your_identity/avoiding_scams_and_hoaxes

This webpage covers common scams and techniques used by scammers and gives useful advice on avoiding being scammed. Although many scams can be recognised by bad spelling and the use of false email addresses, some scams are quite sophisticated.

There are several scams that are recycled each year by scammers.

Nigerian scam: Scams such as the so-called 'Nigerian Scam' distribute emails purporting to be from someone who has a large sum of money that they 'temporarily need help with' ie by using someone's bank account.

This type of plea is used to gain a person's bank account or credit card details. Because of the sheer number of these emails sent out there are always a few people who are vulnerable enough to believe that the scam email is authentic. Most people who work in libraries will see this scam in its various forms.

Dating and Romance scams: Preying on the vulnerable, attempting to get people to divulge personal details and send money. This is still a common scam through which scammers earn millions of dollars a year from Australians.

Scammers are also developing new ways to defraud people eg: **Ransomware:** Individual or company files are encrypted so that users are locked out of their files. Scammers ask for ransom money to allow access to files. The delivery of these scams ranges from malicious email attachments (often zip files), ads on websites or convincing people they need to download apps from unknown sources.

Staff Tip: Recommend to library users to ignore suspicious emails, especially when they contain attachments. Never open the file or download the attached files.

Phishing: Requests for personal or company information by scammers posing as legitimate institutions or businesses. These scams may be carried out via internet or SMS text messaging. Websites may use copied logos and links that look similar to the company's own website address or URL.

Staff Tip: Financial institutions will never ask you via email to provide your personal information and account details.

See more at:

<http://www.scamwatch.gov.au/content/index.phtml/tag/requestsforyouraccountinformation>

Microsoft or Telstra scam: People pretending to be representatives of Telstra or Microsoft call random people saying, 'Your internet account has been hacked' OR 'There is a problem with your internet connection' OR 'Your computer needs fixing'. These scammers are convincing and provide false ringback numbers. Victims lose money from their online banking or bank accounts if they give out their information.

Recognising secure websites

One way of recognising a secure connection is useful, eg: especially for online shopping. In the browser website address bar you should see **https:** and possibly a lock icon instead of the usual **http:** The 's' indicates that the website is encrypting information being sent to and from the website so that computer hackers will not be able to easily access the information.

Clicking on the padlock gives more information about the authenticity of the website.

Privacy

Social media can be fun and useful for information-sharing but can also make people vulnerable to invasions of privacy or at worst can put them into life-threatening situations.

Resources for learning about social media concerns and privacy settings:

http://www.staysmartonline.gov.au/socialising_online

<https://www.staysafeonline.org/stay-safe-online/protect-your-personal-information/social-networks>

Staff tip: Check the privacy settings for all your social media platforms. If you go to account settings on social media websites such as Twitter you can choose various levels of privacy.

Cybersafety for Children

Children can be encouraged to open this site: <http://www.safesearchkids.com/> which is a site set up by Google which helps remove potentially explicit material from appearing in Google search results. It also gives a wonderful explanation of why 'safe search' is important and would be a great resource to recommend to parents.

The **StaySmartOnline** site provides links to resources to assist young people learn about cybersafety and cyberbullying.: <https://www.staysmartonline.gov.au/youth>

Resources

A good starting point for resources relating to cybersafety can be found on the MPLS website:

<http://monlib.vic.gov.au/eLibrary/Our-Training-Notes/Cybersafety>

Some key points to ensure cybersafety:

- Secure passwords (avoid using common passwords such as 1234)
- Consider two factor authentication: <http://lifelife.com/5938565/heres-everywhere-you-should-enable-two-factor-authentication-right-now>
- Anti-virus program installed on computer/devices
- Up to date version of computer software

Staff Digital literacy skills (social media, internet, digital devices)

Being eSmart is a very important part of our role working with the community in public libraries. We will only begin to be eSmart if we have a reasonable level of digital literacy. This means being comfortable engaging with a wide variety of technology and ensuring that we regularly assess our own knowledge and competencies.

Some useful tutorials can be found here: <http://www.gcflearnfree.org/>

This website provides a wide variety of free online tutorials under the banner of Technology. It includes tutorials on: devices, computers (Mac & Windows), social media, Google Cloud, graphics/photos, online safety and general digital skills.

Progressing towards accreditation

The Library Technician will be using the eSmart framework to work towards having the AMR Library Service accredited as an eSmart Library by the end of 2017.

Some tasks will be delegated to staff by the Library Technician.

Each team meeting will include an eSmart component during which the Library Technician will provide an update of our progress, some IT training, or other cyber-related information.