

# Academic Skills for University Success Specialization

## Information & Digital Literacy for University Success



### 5.3a Managing digital identity

#### Security Management Tips

##### Things NOT to do:

- Share passwords with anyone else. At university, you will manage your enrolment and course access with a password, and it's very important to keep this password secure to prevent any tampering with your records.
- Open suspicious\* emails, text messages, files, ads etc.
- Take photos of your ID (government issued licenses, passports, ID, birth certificates etc.) and store them in unsecure places.
- Take photos of your credit cards or bank cards and put them online.
- Use your own, family members or friends' names, pet names, dates, '1234', 'password', '12345678', 'qwerty', etc. for passwords (Burnett, 2015).
- Give bank details online.
- Share personal (full name, address, license numbers, social security numbers, passport numbers, birth date etc.) online.
- Re-use passwords.

##### Things TO do:

- Change your passwords every 6 to 12 months.
- Use a Password Manager like [LastPass](#).
- Never re-use a password.
- Use passwords that:
  - o Are 8 or more characters long;
  - o Use a combination of lower case (aa) and upper case (AA) letters;
  - o Use numbers in combination with letters;
  - o Use symbols such as \*&#^;
  - o Don't have common dictionary words ("dragon").
- Report suspicious emails as spam (through your email address, or government services like <https://www.scamwatch.gov.au/>).
- Verify people's identity through an independent search (not just their contact details in an email) if they contact you online.
- Make sure a website is secure when giving details: always look for a  or  symbol in the address bar (Chrome and Firefox, respectively).

\*suspicious = from people you don't know, or companies you haven't specifically signed up to.

# Academic Skills for University Success Specialization

## Information & Digital Literacy for University Success

### 5.3a Managing digital identity

#### References and additional resources

- Australian Competition and Consumer Commission. (2015, May 14). Identity theft [Text]. Retrieved June 17, 2016, from <https://www.scamwatch.gov.au/types-of-scams/attempts-to-gain-your-personal-information/identity-theft>
- Burnett, M. (2015, January 22). Is 123456 Really The Most Common Password? — XATO: SECURITY. Retrieved June 16, 2016, from <https://xato.net/is-123456-really-the-most-common-password-51cd4259927d#.o5s2v5sgZ>
- Goodin, D. (2012, August 21). Why passwords have never been weaker—and crackers have never been stronger. Retrieved June 17, 2016, from <http://arstechnica.com/security/2012/08/passwords-under-assault/>
- Gosney, J.M. (2016, June 1). How LinkedIn's password sloppiness hurts us all. Retrieved June 17, 2016, from <http://arstechnica.com/security/2016/06/how-linkedins-password-sloppiness-hurts-us-all/>