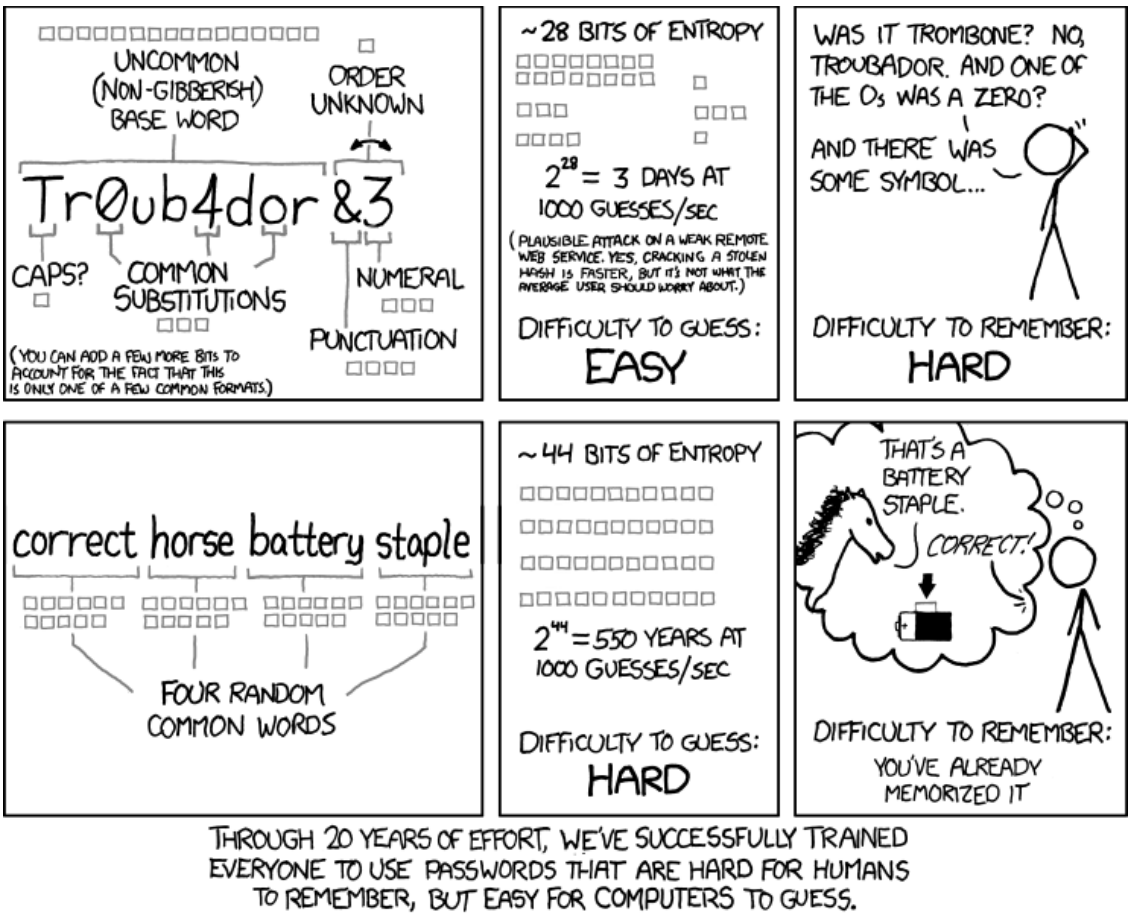
Stay Smart Online Week 2015 Day 1

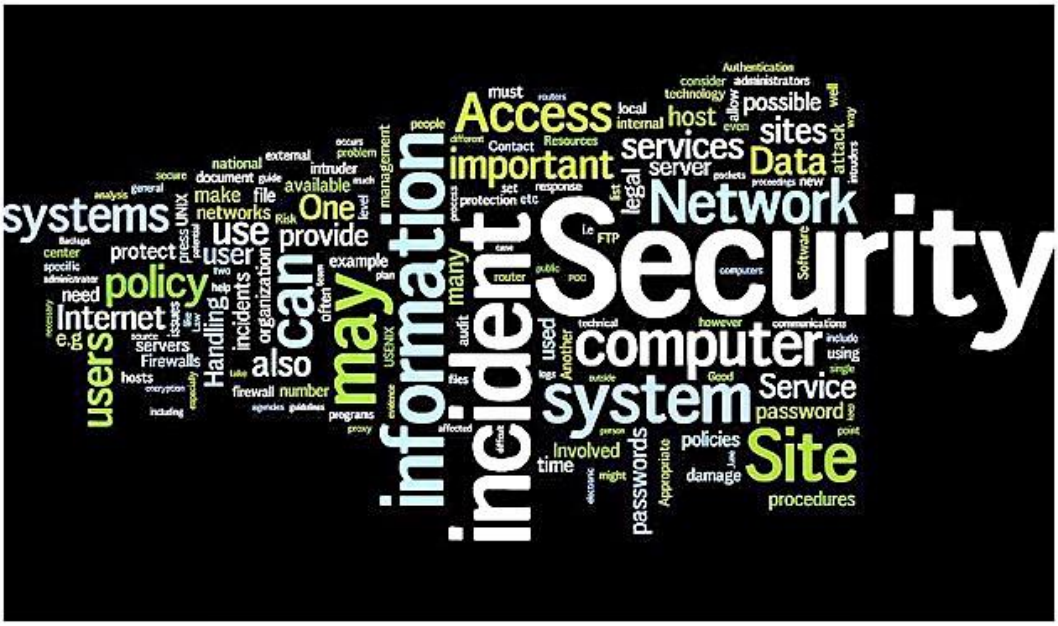
To make our engagement online and that of our customers that much easier, here are some tips to keep in mind (there will be one each day for the rest of the week!).

On passwords:



- Passphrases are better than passwords – the longer the better.
- Avoid repeating passwords – if one get compromised, all accounts that use that password can be compromised (try this link to see if your account has been compromised)
- More characters are better (bigger the set of character, longer the algorithm has to run)
- Avoid information that people can find/guess about you (pets, birthdays etc)
- Use partial words or words that will not be found in a dictionary (or at least are uncommon enough to not be in the Shorter Oxford)
- If you must write something down, write down password hints, not the passwords themselves: Consider a password manager
- Keep a list of all accounts so that if one is hacked you can manage the rest

Stay Smart Online Week 2015 Day 2 - Security

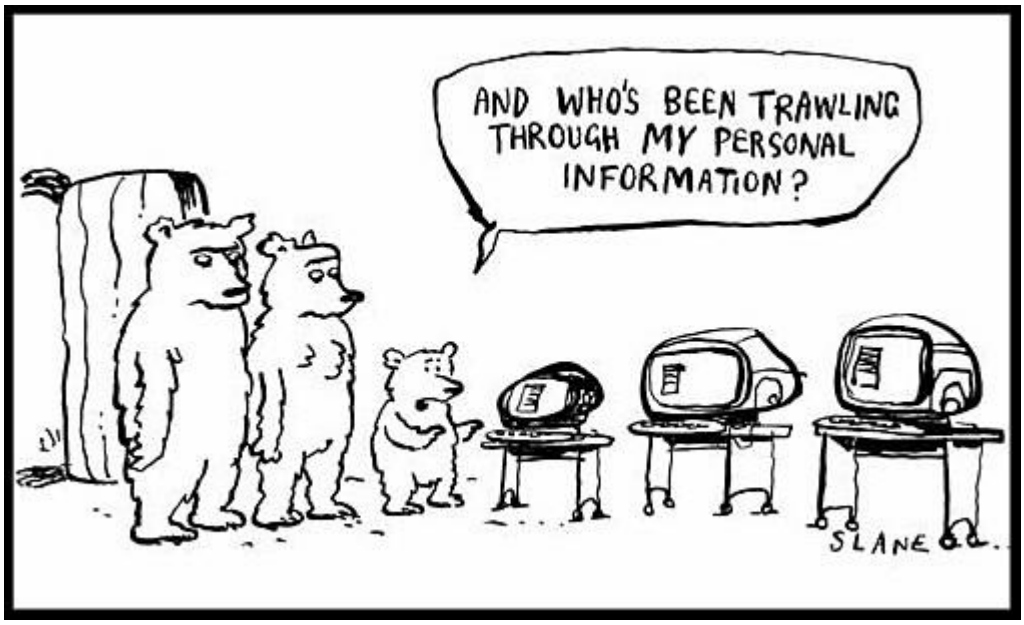


What assets are you trying to secure? What are the threats? How can you avoid/mitigate them?

- Ensure the physical security of your device by not leaving it lying around
- Remember that security applies to desktop, laptop as well mobile devices
- Register your devices/ keep your receipts in case of theft
- Have a master lock on your laptop/device (remember this one!)
- Turn on your firewall
- Have an antivirus software package installed – considerations here
- Back up your devices
- Have a disk cleaner and use it regularly
- Keep your operating system and apps up to date – automatic updates recommended
- Stay up to date with scams – staysmartonline alert service is excellent
- Paying money does not necessarily mean the package is better
- Be careful when looking for accurate neutral reviews on the net – use trusted sources
- USBs can be compromised – keep minimal information on them and keep them secure
- Encryption is an option, but only if you are willing to learn enough to make it effective

Stay Smart Online Week 2015
Day 3 - Privacy

What personal information do you want to keep private, and from whom? Where does your personal level of comfort lie on the 'ease of use' Vs 'total privacy' spectrum?



- Decide the level of privacy with which you are comfortable
- Get to know your privacy settings
- Regularly manage the security settings of apps you are on (they will change often and without warning, especially after updates)
- If you aren't using an account, make it invisible, suspend it or delete it
- Only post information you are comfortable with the world having access to
- Manage who has access to what through your privacy/security settings
- Only post information you have the authority to post (get permission before posting photos/content about your sister/granddaughter etc.)
- Use stealth browsing if you want to remain untracked
- Delete cookies regularly – also clear your cache
- Decide what information needs to be kept private and create systematic barriers between that and everything else (talk to journalistic sources via secure chat on ToR, use gmail chat for conversations about kittens)
- Remember no information is anonymous once you enter any identifiable data
- Consider when and which accounts should be linked and why
- Consider encrypted communication for sensitive materials (estate documents etc)
- Save messages as pdf not word – computers can scan for text more easily than cursive handwriting or pdfs

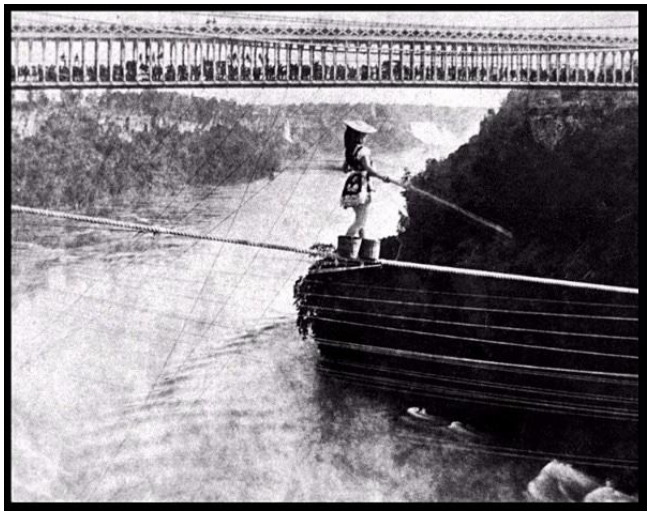
Stay Smart Online Week 2015
Day 4 - Browsers & Plug-ins

Plug-ins/browser customisations for the security conscious! Most of these plug-ins are available for all major browsers. Where they aren't, explore alternatives that perform the same function.

- Pick your browser well. Not all of them are created equal – some are specifically security focussed (e.g., Tor) some can be customised to be (most major ones)
- Set your browser to update automatically
- HTTPS everywhere – courtesy of the EFF and the Tor Project, and generally awesome!
- NoScript – to manage executable content (helps prevent JavaScript, Flash etc based scripted attacks)
- Adblock Plus – to manage advertisements (you can create your own white/black lists)
- Disconnect – to prevent third party tracking
- Web of Trust (WOT) – basic security crowdsourced to provide ratings for links and URLs
- LongURL – to make the clicking of shorterned embedded links more secure
- Lastpass – or any other password manager that works for you
- duckduckgo – reigning favourite as default search engine (defaults to more private rather than less)

Stay Smart Online Week 2015
Day 5 - Talking to the public about security & privacy(and tech generally)

We have a responsibility to encourage and foster the safe, smart and responsible use of technology with our customers. And to do this is in a customer focussed and respectful ways.



Some tips to keep in mind:

- Acknowledge the limits of your knowledge/expertise
- Own your opinion and always clarify that that is one of many differing opinions
- Provide a neutral or at least balanced picture
- Focus on showing where to find information and how to judge its suitability as opposed to providing an answer
- Offer no input into what decision should be made – offer input on what information could go into making the decision and where that might be found
- Let them make changes – avoid taking their device/account and doing it yourself – that way they can make their own decisions and manage the consequences
- Ask for permission to look at their device or account and remind them that you will be clearing that information at the end of your interaction
- Tech information changes quickly – what may have been correct last week may no longer hold true – focus on finding out together