

1. This section is worth 100 points toward the final. Please put all the required documentation in a pdf file called /section01.pdf/.

1.1. Create five different short "elevator phrase or phrases" about important security concept(s) for your family or friends. An "elevator phrase" is a very short and to the point saying that can be delivered in 5-10 seconds and repeated many times.

Think before you click.

Passwords: Longer is Stronger.

Prepare for Disaster: Recover Faster.

There's no excuse for computer misuse.

Control + Alt + Delete, When You Leave Your Seat

1.2. Identify a unique security incident that support each one of your family/friends "elevator phrase or phrases". Provide a short description (a paragraph or so) of the incident, and a link for additional information about the incident that supports the phrase or phrases.

Think before you click.

This happens all the time, people overshare or hand out information online without thinking anything of it. Scams, malware, and viruses can all be sent to your inbox and if you're not careful enough, you can click a link or open a file and cause all sorts of damage to your computer.

<https://www.onguardonline.gov/media/video-0002-heads-stop-think-click>

Passwords: Longer is Stronger.

Short passwords are easy to crack. In fact, a lot of people are guilty of using the same very common and simple passwords. In the past I have used Backtrack (now Kali) to crack Wi-Fi passwords. Google is littered with information on how to do this very simple (for an experienced user, I suppose) task.

<http://lifel hacker.com/5305094/how-to-crack-a-wi-fi-networks-wep-password-with-backtrack>

Prepare for Disaster: Recover Faster.

Who hasn't had a Hard Drive or Memory card of some sort crash? Are even broke a phone and lost all their contacts, photos, and whatever else vanish forever? Luckily now, Google and sites like Dropbox allow for an automatic backup of all your information and data. I can even consider myself guilty of not creating a backup and making this terrible mistake. Not anymore!!

<https://www.dropbox.com/>

<https://accounts.google.com/>

There's no excuse for computer misuse.

A 21-year-old named Gareth Cross was given a 12 month sentence after hacking into a private Facebook account. In January 2011, Cross gained unauthorized access to the Facebook account an individual including the private email function. The breach was report to the FBI who traced the source back to the UK.

<http://thenextweb.com/uk/2012/05/17/uk-facebook-account-hacker-hit-with-12-month-prison-sentence/>

http://www.sqa.org.uk/e-learning/ITLaw01CD/page_03.htm

Control + Alt + Delete, When You Leave Your Seat

You should always lock your account when you walk away from your computer. This should be common sense to keep all your information locked and private. Personally this isn't any different with a phone. A user could leave his desk with their bank account information up and anyone walking by could cause all sorts of damage.

http://ask-leo.com/is_leaving_a_website_open_on_my_computer_dangerous.html

1.3. Provide a security policy or procedure related to each "elevator phrase". Identify the source of each security policy or procedure.

Think before you click.

Do not click random links: Do not click any link that you can't verify. To avoid viruses spread via email or instant messaging (IM), think before you click; if you receive a message out of the blue, with nothing more than a link and/or general text, do not click it. If you doubt its validity, ask for more information from the sender.

<https://kb.iu.edu/d/akln>

Passwords: Longer is Stronger.

Enforce password history, maximum password age, minimum password age, minimum password length, passwords must meet complexity requirements, store passwords using reversible encryption for all users

<https://technet.microsoft.com/en-us/magazine/ff741764.aspx>

Prepare for Disaster: Recover Faster.

Create and document a data backup policy. Decide where backups are stored, who can access them, how often data is backed up, what kind of backups are performed, and what hardware and software are recommended for performing backups.

<https://www.dataone.org/best-practices/create-and-document-data-backup-policy>

There's no excuse for computer misuse.

Encrypt files, Use strong passwords, lock your computer when you are away from it, and always shred printouts that contain sensitive data.

http://www.igcseict.info/theory/7_2/misuse/

Control + Alt + Delete, When You Leave Your Seat

Lock Your Desktop With a Password-protected Screensaver

Windows 7

1. Right-click on your desktop.
2. Select **Personalize**.
3. At the bottom of the window that opens, click **Screen Saver**.
4. In the *Wait* box, set the amount of time your computer can be inactive before the screen saver turns on. For security reasons, a short amount of time, like 5 minutes, is best.
5. Check the box that says **On resume, display logon screen**.
6. Click **OK**.

Mac OS X

1. Click the **Apple** menu.
2. Click **System Preferences**.
3. Click on **Desktop & Screensaver**.
4. Click the Screen Saver tab, and set the amount of time your computer can be inactive before the screen saver turns on. For security reasons, a short amount of time, like 5 minutes, is best.
5. Click **Security and Privacy**.
6. In the General tab, check the box **Require password to wake this computer from sleep or screen saver**. For security reasons, set it to a short time, 5 seconds or less.

Lock Your Desktop Manually

Windows 7

Simply hold the Start (Flag) button and hit the L button.

Mac OS X

1. Set up a [Hot Corner](#) on your desktop.
2. Navigate to the Hot Corner to activate the screen saver.

<http://weill.cornell.edu/its/security/secure-computing/safeguard-your-data/lock-your-desktop-when-youre-away.html>