How secure are you online?

The checklist:

• Use strong passwords both for your College accounts and all your personal accounts such as Facebook, Twitter, Amazon, PayPal

• Don’t use the same password for everything; this increases the likelihood of multiple accounts getting hacked at once potentially turning a small problem into a disaster!

• Don’t let the software installed on your computers fall too far out-of-date. This goes for antivirus applications in particular – they are only truly effective when up-to-date.

• Be aware of scams; don’t reply to emails or pop-up messages in your browser that ask for passwords or personal or financial information.

• Have you backed up your important data recently? Avoid disaster by coming up with a data and devise backup strategy now. Concentrate on your most important information and come up with a plan to back it up regularly.

Phishing awareness

• Always remember that IS Services will never ask for username and password information through an email

• Be extra vigilant about not opening unexpected emails
Guidelines for securing your mobile device

- Set a password or Personal Identification Number (PIN) on your device.
- Make sure your device automatically locks if it has not been in use for a set period of time.
- Keep the software and apps up-to-date just as you would with your laptop.
- Disable Bluetooth when not in use and switch Bluetooth devices to hidden mode.
- Make sure to delete all information stored on your phone or tablet prior to discarding it.
- Back up and secure your data.

Keep your accounts secure with strong passwords

It can be tempting to reuse a single password for multiple online accounts, like Facebook or Twitter, but this is never a good idea. Password reuse creates a security vulnerability which could provide an attacker with easy access to many of your accounts and compromise a vast amount of your information.

How do I create a strong password?

The key ideas to think about when creating a password are: length and complexity. You can always test your password with a reputable online password checker (try http://www.passwordmeter.com).

The chart below illustrates a handy way of constructing a strong password.

<table>
<thead>
<tr>
<th>What to do</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>First start with a memorable sentence</td>
<td>I heart teddy bears</td>
</tr>
<tr>
<td>Then remove the spaces between the words in the sentence</td>
<td>iheartteddybears</td>
</tr>
<tr>
<td>Next capitalise the first letter of each word</td>
<td>IHeartTeddyBears</td>
</tr>
<tr>
<td>Turn words into short-hand or intentionally misspell a word</td>
<td>IHrtTddyBrs</td>
</tr>
<tr>
<td>Finally add length and complexity with special characters and numbers</td>
<td>%IHrtTddyBrs76</td>
</tr>
</tbody>
</table>

NEW mypassword.tcd.ie

If you ever forget your password, this service will enable you to change it easily and remotely by visiting mypassword.tcd.ie. With this service, you will be able to change your network login and MyZone password from anywhere, through a web browser, have details sent to your mobile phone and confirmation emails sent to an email address of your choice.