Hand-out: do : Nothing (social media security settings with Facebook used in examples)

University of Oxford Information Security infosec@it.ox.ac.uk:
www.it.ox.ac.uk/infosec/protectyourself/socialmedia/

"Social engineering" is a way of fooling you into disclosing information. It's nothing new, but with social media sites like Facebook, it has become easier than ever to harvest personal information from unsuspecting targets. By obtaining personal information from your account - simple details like your birthday, your phone number, or your location - hackers might be able to unlock the "account recovery" features of your other online accounts. This might eventually lead to your credit card information or your identity. A "ladder of access" can be put together. It's common sense but the information you should never give out on social media games or quizzes includes:

- Mother's maiden name
- Personal banking details
- Password
- Other Personally Identifiable Info (PII) where you live, social security or phone number.

Ask yourself "If someone was out to get me, my family, or my department, could any of this information help them?"

Social Media is a target for "social engineering attacks". But you can:

- 1. Set up Login Approval to keep attackers out of your account
  - Use a strong and unique passphrase
  - Set up Trusted Contacts to help you when you get hacked
- 2. Use secure Web connections https://
- 3. Secure your privacy settings (and don't overshare, and don't expect anonymity)
- 4. follow social media guidelines to protect other staff and readers
- 5. know what to do if hacked!

1. The examples in this hand-out use Facebook, the principles are the same for blogs, YouTube, Twitter, Google+ and Gmail, etc.

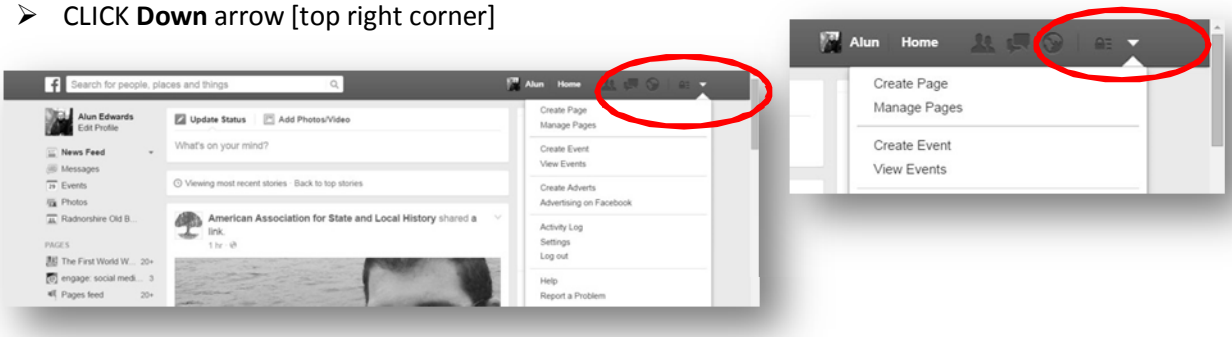
Go to an Internet browser on the computer and enter www.facebook.com/ in the Web address bar.

Login to Facebook.

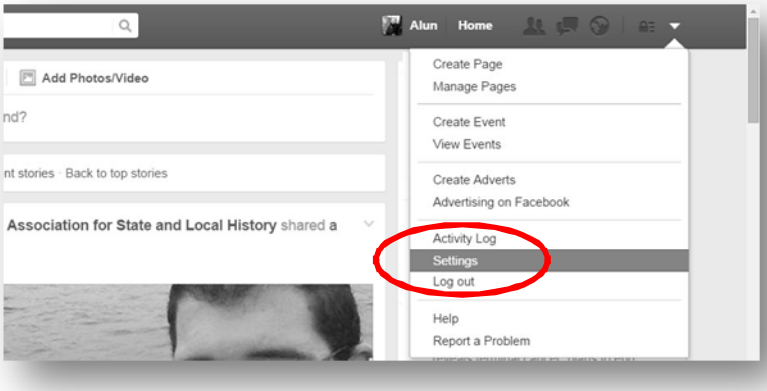
1a. Set up login approval for Facebook

Login Approvals is Facebook's two-factor authentication feature (an added layer of security that requires a code to be entered to complete the login process if Facebook doesn't recognise this device). When you're logged in to Facebook:

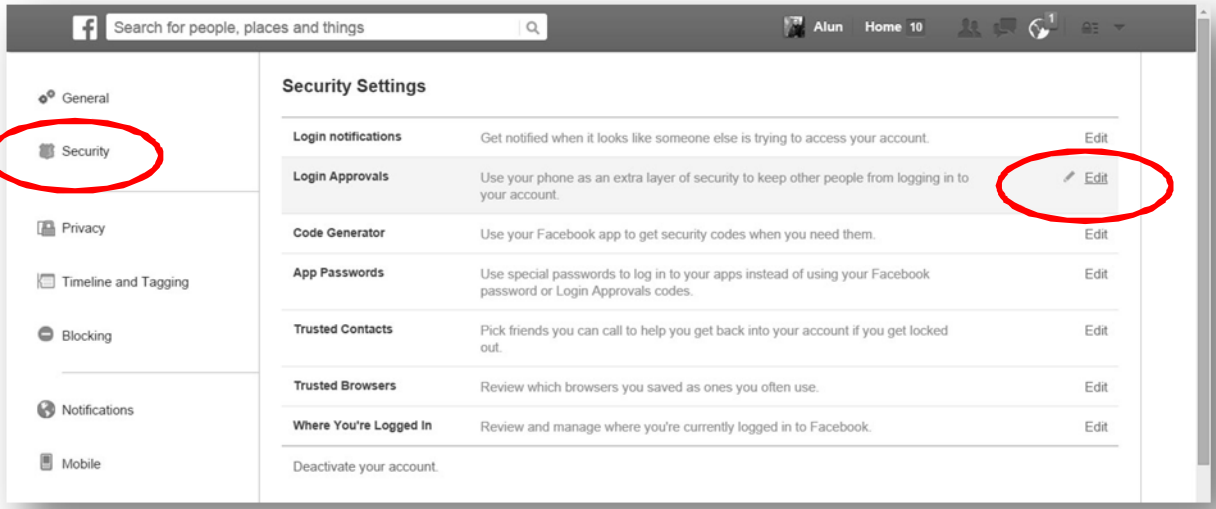
- CLICK **Down** arrow [top right corner]



- CLICK **Settings** [near the bottom of the menu]



- CLICK **Security** [left hand menu] >> main menu: **Login Approvals** >> CLICK **Edit**



- Then check box "**Require a security code to access my account from unknown browsers**" [An "unknown browser" is a computer or phone you haven't used before]
- Follow the instructions, e.g. identify devices or your mobile number
  - And to enter the 6-digit PIN texted to you
  - And if you also have Facebook as an app on your tablet or phone, instead of texting you the secret code the Facebook app will generate a code for you to use. To do this, from the **Security** settings screen: CLICK **Edit** next to **Code Generator**.
  - And you can print a list of codes. Click on the **Get Codes** link in the **Login Approvals** section. A printed list will be helpful if:
    - you know that you aren't going to have access to your phone
    - mobile signal is poor
    - you are traveling
    - your phone dies a lot
  - And to get notified when it looks like someone else is trying to access your account CLICK **Edit** next to **Login notifications**.

You should set-up two-factor authentication on any sites that offer it: including Twitter, Google/Gmail, LinkedIn, etc. This means a hacker has to have not only your username and password, but to also have access to your mobile device.

Use a dedicated email address for Facebook

If you use an email account that you also use for banking or other sensitive information, then all of these are at risk if your Facebook account is ever hacked. Change to a new email address from one of the free email providers like gmail.

Use a strong and unique passphrase on Facebook

Don't use the same passphrase on any other account - you MUST not use your Oxford passphrase!

For help in choosing a strong passphrase see
http://www.it.ox.ac.uk/infosec/protectyourself/passwords/

1b. Set up Trusted Contacts in Facebook

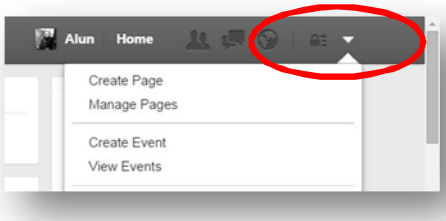
This lets your friends help you if you're having trouble logging into your account - maybe you forgot your passphrase or worse you've been hacked - it's an account recovery feature.
Choose 3-5 people:

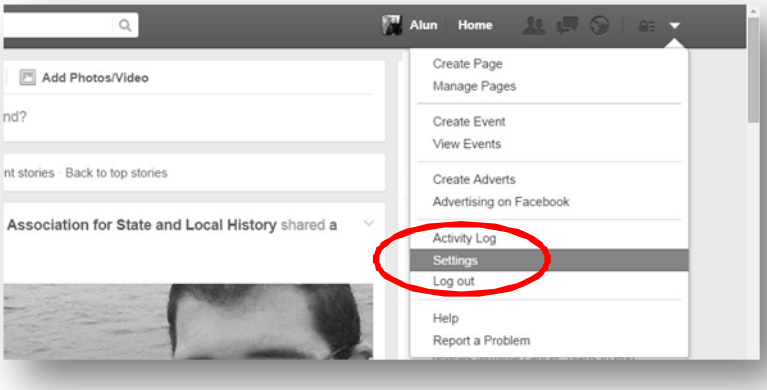
- who use Facebook frequently;
- you trust, like friends you'd give a spare key to your house;
- who are not likely to lock you out of your account for a joke!
- you can reach without using Facebook, ideally over the phone or in person, since you'll need to contact them when you can't log in.

The more friends you choose, the more people who can help you when you need it.

Go to the **Security** menu (find out how in 1a. above) i.e.:

- CLICK **Down** arrow [top right corner]
- CLICK **Settings** [near the bottom of the menu]



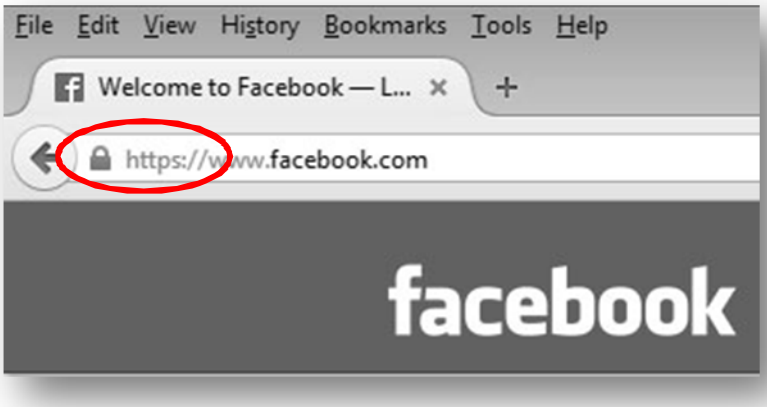


- CLICK **Security** [left hand menu] >> main menu: **Trusted Contacts** >> CLICK **Edit**

2. Use secure Web connections https://

Be careful when using public Wi-Fi spots and public computers (hotel foyer etc.). Pay close attention when asked to sign in online. Most importantly, check to see if the Web address begins with https:// The "s" means that your connection to the website is encrypted and more resistant to snooping.

Facebook uses **https** by default. So if https does not display in the Web address or a padlock is not visible (in some Internet browsers this could be on the left or the right of the address) then logout.



3. Be more mysterious and secure your privacy settings

3a. Be careful what you post, where you post, and when:

- Don't over share, e.g. on holidays
- Think about your children's safety (and their future digital identity)
- Beware of shoulder-surfing (when someone watches you and can see you enter your password etc.)

3b. Reputation

E.g. 1OneMinuteNews on YouTube: http://youtu.be/s-QIN0rsb5I

3c. Can you spot a social media hoax?

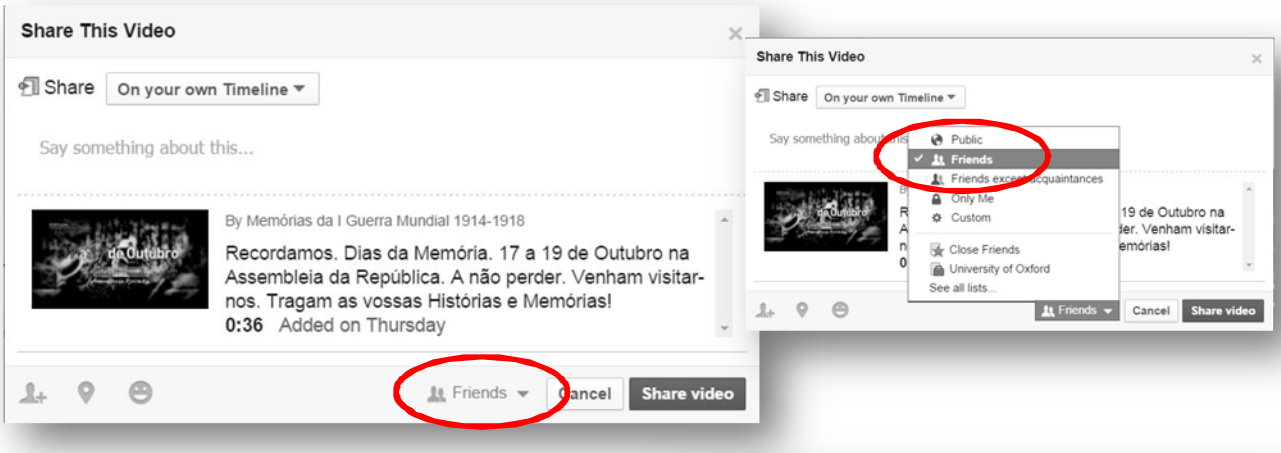
Beware of social media hoaxes. The worst of these hoaxes are attempts to gain access to your data. Your Facebook could get hacked or your account could be used to trick your friends.

Be suspicious of everything on Facebook and surf the Internet defensively. Don't click a link which says “Hey is this really a picture of you?” Spot key phrases used in scams like sentences that begin with “Did you know...?” and “Can you believe...?” These phrases entice you to click when you probably shouldn't.

- Never enter your password.
- On Facebook follow www.facebook.com/facecrooks and www.facebook.com/snopes/
- Check if a post is a hoax or a scam e.g. by entering some of the text in a search engine, or www.snopes.com or www.facecrooks.com and other guides.

3d. Future posts and posting now

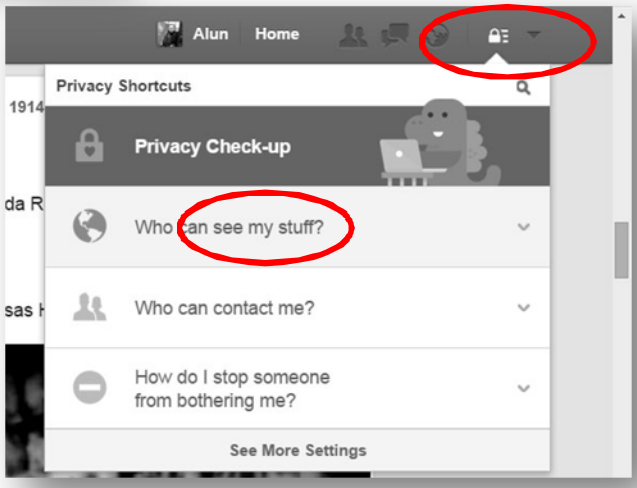
3d. i. When you post or change your “About” on Facebook you should check that the audience setting is set to **Friends** or something more restrictive. (Exceptions will be when you’re using Facebook as an engagement channel for work.)



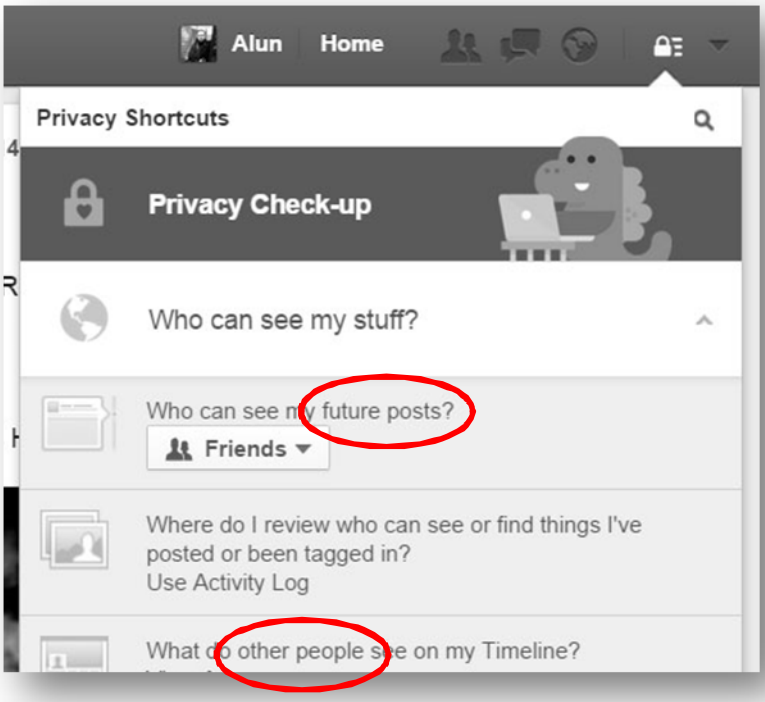
3d. ii. To change who can see your future posts to **Friends** -

When you’re logged in to Facebook:

- CLICK **Padlock** [top right corner]
- >> CLICK **Who can see my stuff?**

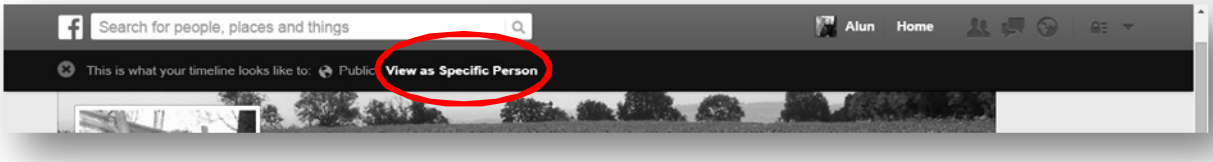


- CLICK **Friends** at **Who can see my future posts?**



3d. iii. To see what your timeline looks like to a specific friend:

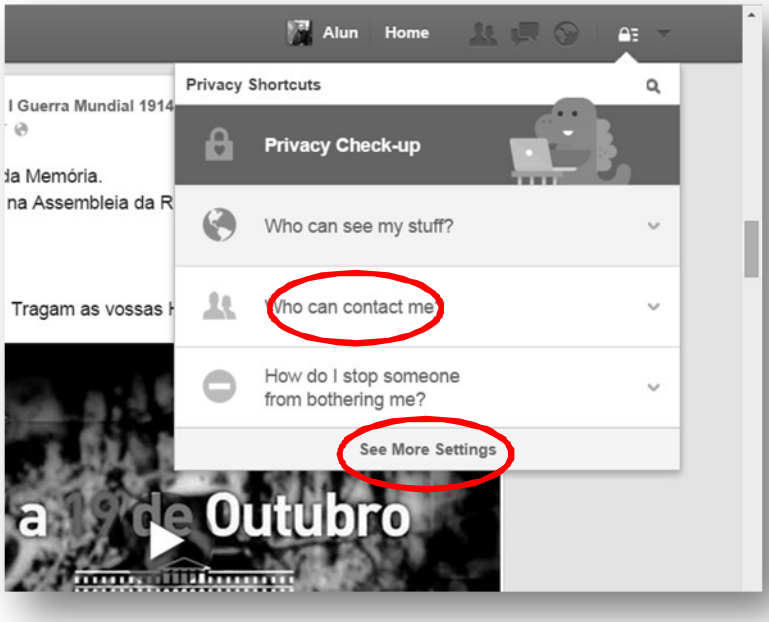
- Click **What do other people see on my Timeline?**
- This lets you see what your timeline looks like to the Public
- And you can type in the name of a specific friend over the words **View as Specific Person**



3e. Set other Privacy settings

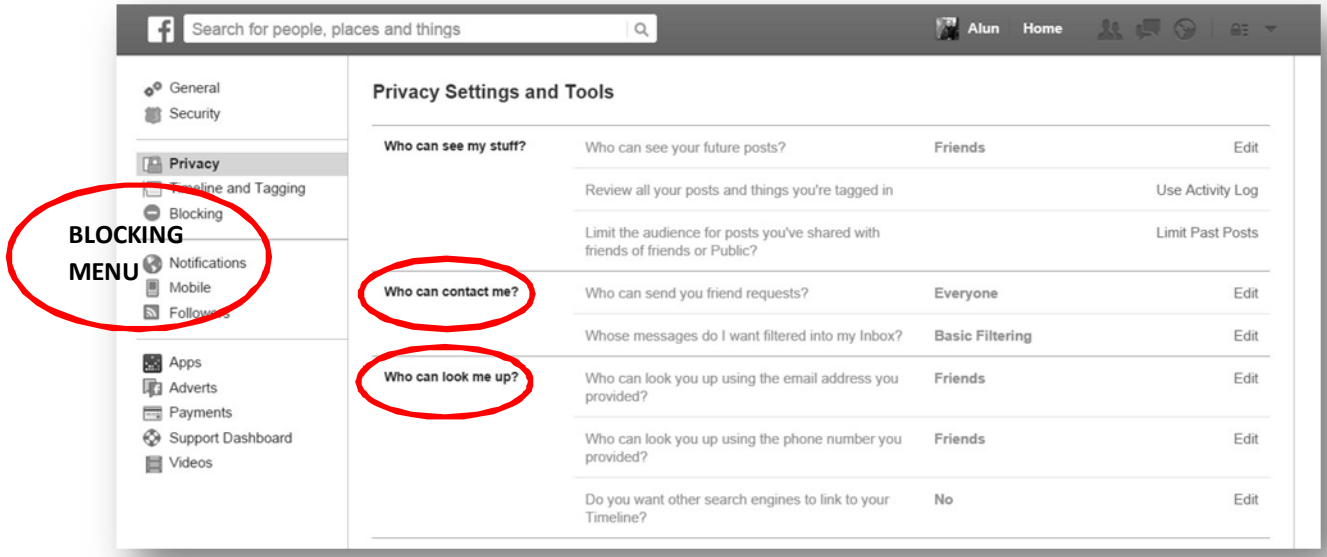
3e. i. When you're logged in to Facebook:

- CLICK **Padlock** [top right corner]
- CLICK **Who can contact me?**
- Set who can **send you friend requests**. If you want people from your past to be able to locate you, then you'll have to set this to Everyone.
- Select if you want **Basic** or **Strict filtering** for your inbox.
- Learn how do you **stop someone from bothering** you?



3e. ii. Then CLICK **See More Settings**: (screenshot overleaf)

- Set **Friends** for **Who can look you up using the email address you provided?**
- Set **Friends** for **Who can look you up using the phone number you provided?**
- Set **No** for **Do you want other search engines to link to your Timeline?**

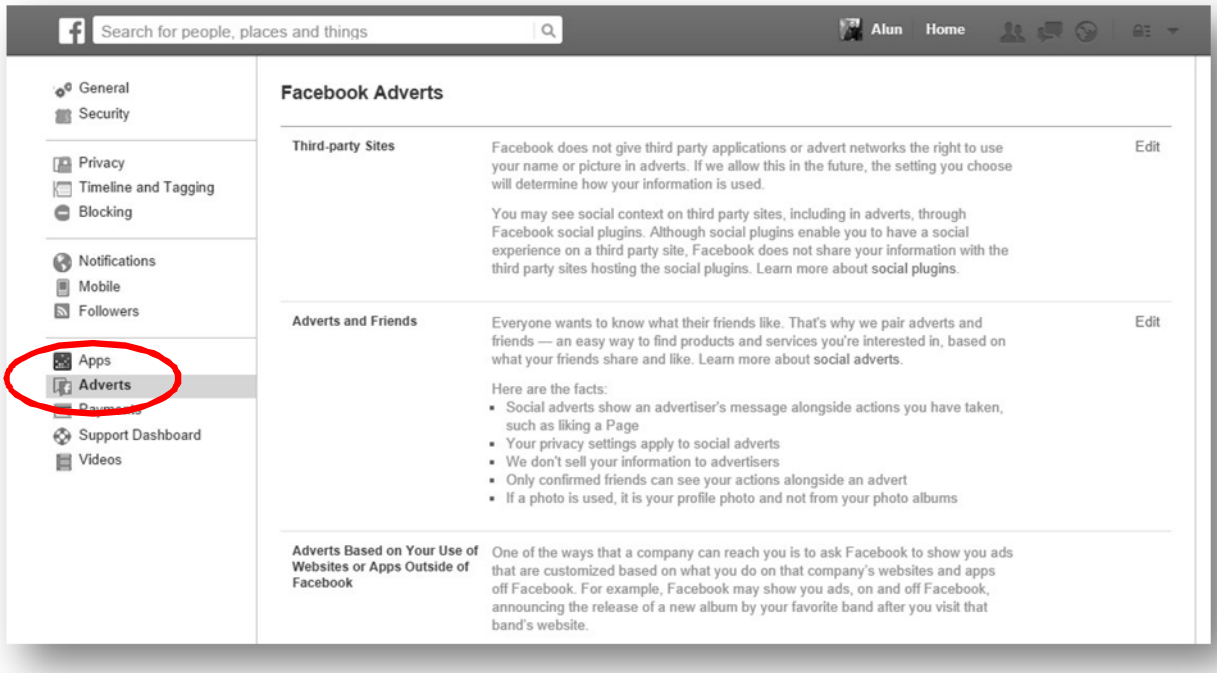


3e. iii. Then CLICK **Blocking** in the left hand menu (screenshot above):

- Set the **Restricted List** for friends that you only want to share public items with.
- Set the **App blocking** options to restrict invites from annoying applications and friends.
- **Block users** to stop someone from seeing your posts, from tagging you, inviting you, & chat.

3e. iv. Then CLICK **Adverts** in the left hand menu

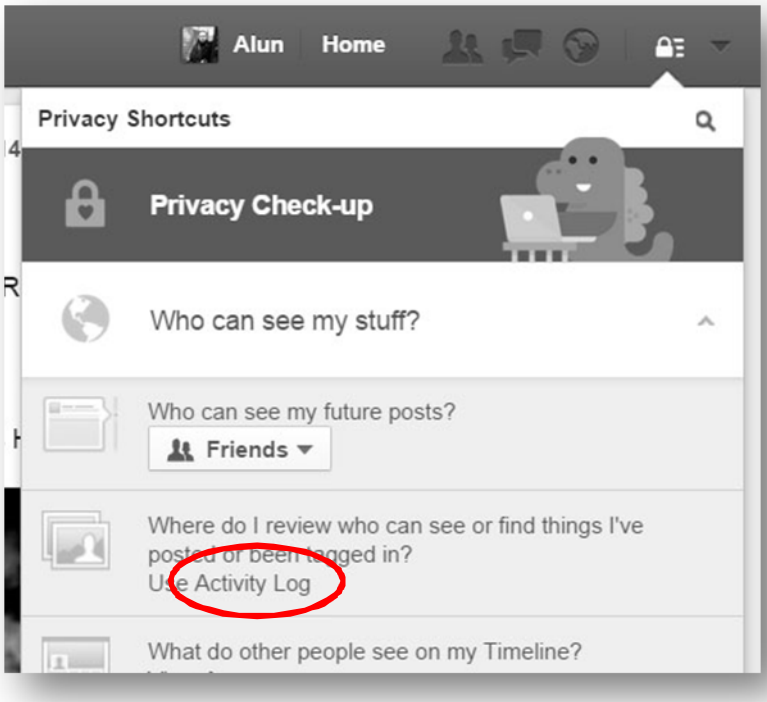
- Edit these settings to **No one**
- Click **Opt out** on the section about Adverts Based on Your Use of Websites or Apps Outside of Facebook



3f. Review your past

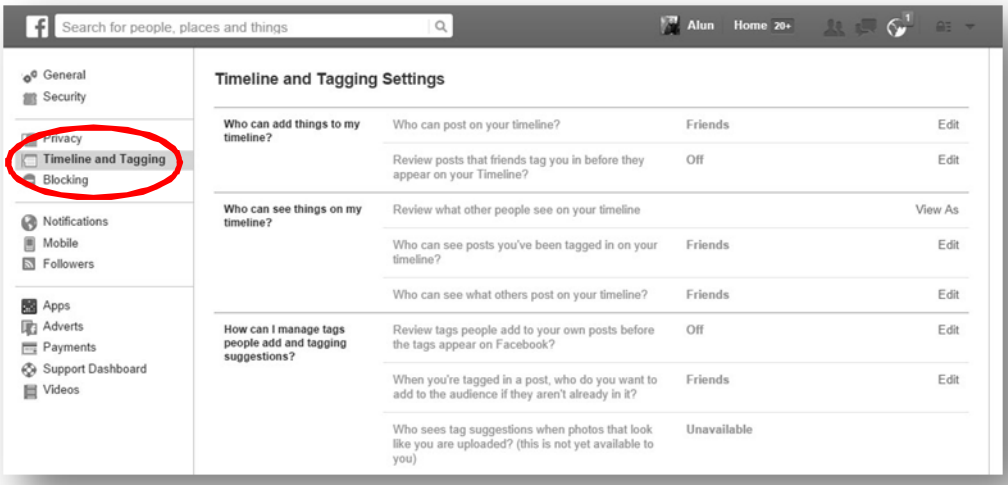
Use **Activity Log** to view your posts, what you've been tagged in, photos etc.

- You can edit, or delete individual items
- You can look at ALL photos for example, and change the audience settings for all
- When you delete remember that if something has been online for only a little while copies may exist somewhere else



3g. & 3h. Change in your privacy settings how you want friends to tag you or post on your timeline

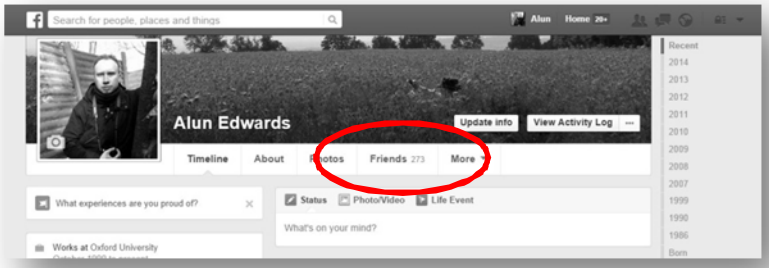
- CLICK **Timeline and Tagging** in the left hand menu
- Edit **Who can add things to my timeline?**
  - Edit **Who can post on your timeline?**
  - Edit if you want to **Review posts that friends tag you in before they appear on your Timeline?**
- Edit **Who can see things on my timeline?**
- Manage tags people add and tagging suggestions:
  - Edit **Review tags people add to your own posts before the tags appear on Facebook?**
  - Edit **When you're tagged in a post, who do you want to add to the audience if they aren't already in it?**
  - Edit [may be unavailable] **Who sees tag suggestions when photos that look like you are uploaded?** (this is something like facial recognition)

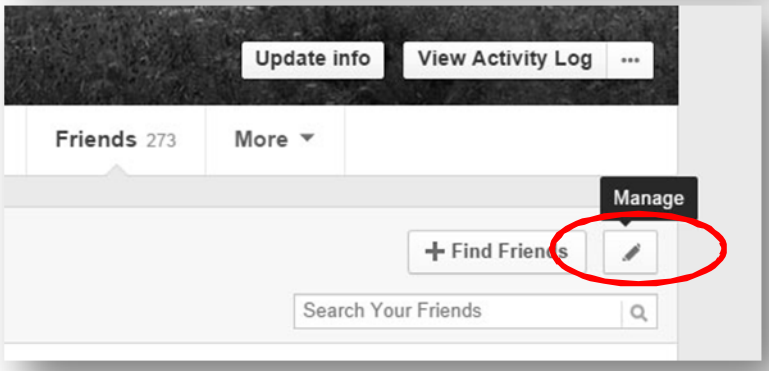


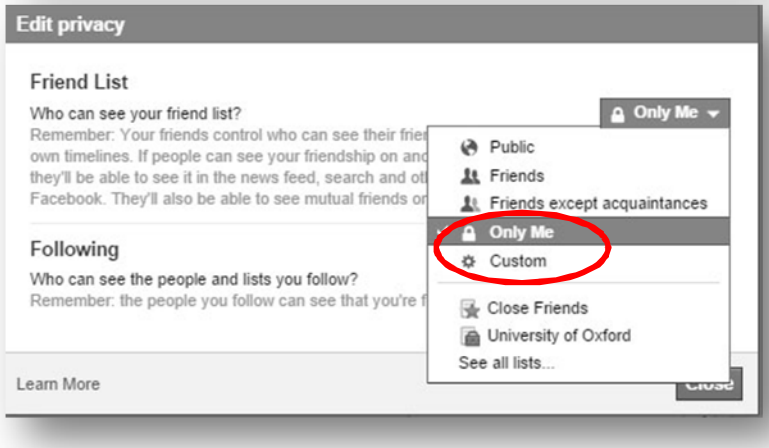
3i. Set your friend list visibility to 'Only Me'

When cyber criminals hijack a Facebook account they extract as much data as possible for identity theft, and fraud, and to search for more victims. E.g. they could create cloned profiles of your account and then target everyone on your friends list. Similarly, you protect yourself a bit more when a friend's account is hacked.

- Go to your timeline
- CLICK **Friends** (below your cover image)
- CLICK the **pen icon** to Manage your friend list
- CLICK **Edit Privacy**
- CLICK **Only Me**

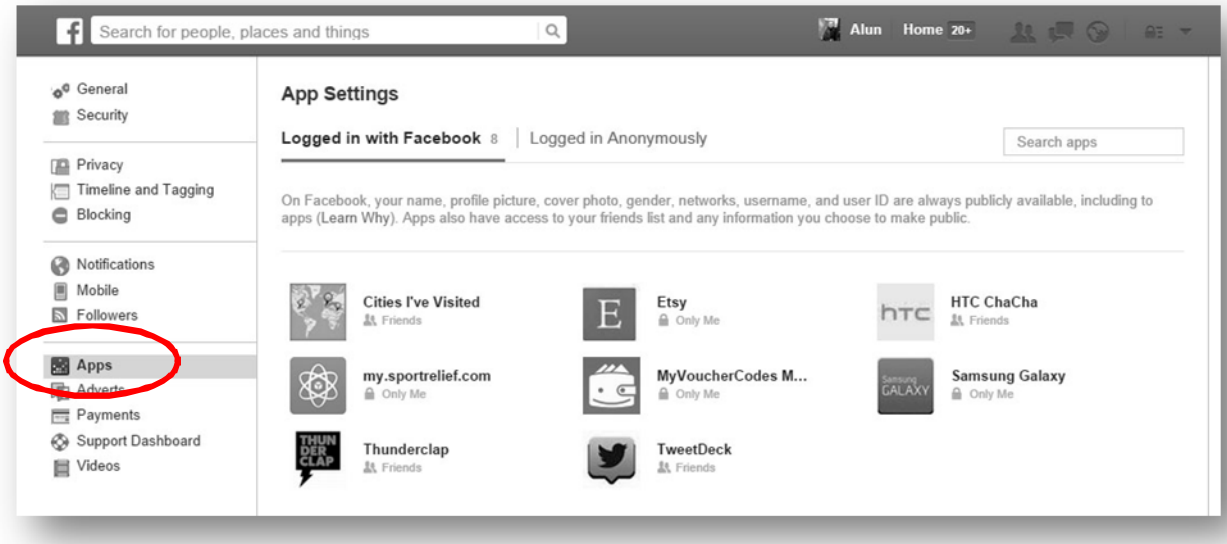




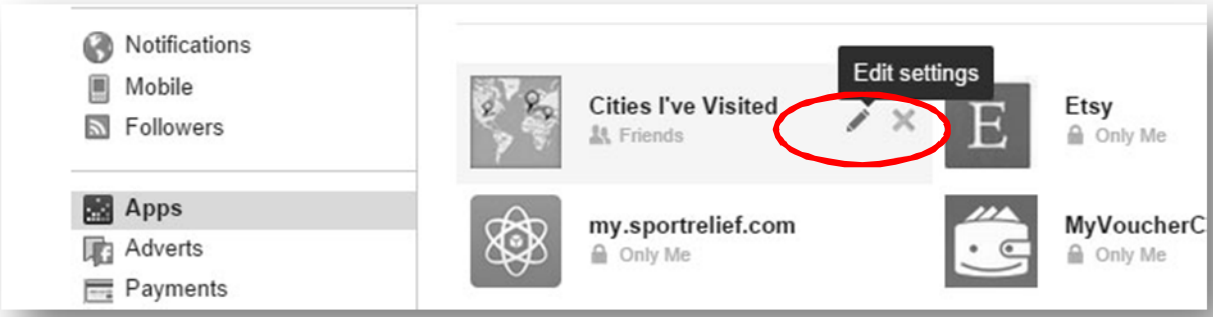


3j. Manage your apps

- Go to the **Settings** menu
- CLICK **Apps** in the left hand menu



- Move your mouse over an app
- CLICK the **pen icon** next to the app to **Edit Settings**



- For every app:
  - Toggle through the detailed settings
  - E.g. what apps you're using outside of Facebook
  - E.g. control the personal information that other apps can obtain
  - E.g. review the privacy settings on posts made with older versions of Facebook's mobile apps
- Delete any app which appears too invasive
- Delete any app you don't use anymore

If you use Facebook on a phone or a tablet consider the permissions and terms of use that the app Facebook Messenger requires, e.g. see http://facecrooks.com/ and search for **messenger**

3k. Install an ad-blocker on your Internet browser

E.g. in the Google Chrome browser go to the **settings icon** (like a menu with multiple horizontal lines). Scroll down to **Settings.** Clicks **Extensions** in the left menu. Click **Get more extensions** and search ad-blocker. Try AdBlock Plus or one of the others.

4. Social media policies and response guides

There are **guidelines** about social media:

- "Online Social Networking" by UK government authorities ESG and CPNI http://www.cpni.gov.uk/documents/publications/2010/2010032-gpg_online_social_networking.pdf
- "Social Media for Staff Policy Template" by Jisc Legal http://jiscleg.al/smediapolicy
- There are social media guidelines in preparation by HR policy writers at the University of Oxford, and by UCISA.

IT Services offers advice on engaging online with your audiences. For example you can adapt the suggestions about moderating comments in your blog and protecting your readers from spam and worse to most social media platforms:

- Creating a WordPress Site - securing your blog: https://creatingawordpresssite.wordpress.com/category/security/ e.g. Set roles for the team, with more than one trusted person as admin (and all admins should enable 2-factor authentication): https://creatingawordpresssite.wordpress.com/2015/01/30/assign-different-roles-

to-people-who-contribute-to-your-blog/ and moderate comments and label tolerance level for negative responses: https://creatingawordpresssite.wordpress.com/2014/06/09/protect-your-blog/

- Ideas for how to cope with trolls, online bullying and sexual harassment, including Creating a better Internet together! In the Education Enhancement Team Blog: https://blogs.it.ox.ac.uk/eet/2014/02/13/creating-a-better-internet-together/

5. What if you're hacked?

The Information Security team are beginning to gather advice on our website, as well as providing some guidance for social media use in work: http://help.it.ox.ac.uk/service/information-security

If you entered your social media password on the wrong site, there is help out there! Immediately you MUST go to a different trusted computer and change your account's password, and you MUST contact your local IT support.

Twitter:

- https://support.twitter.com/articles/185703-my-account-has-been-hacked
- https://support.twitter.com/articles/31796-my-account-has-been-compromised

Facebook:

- to report your account has been hacked https://www.facebook.com/hacked
- Facebook help centre https://www.facebook.com/help/131719720300233/
- and **Facecrooks guides** include:
  - Four Things You Need To Do If Your Facebook Account Gets Hacked http://facecrooks.com/Safety-Center/Four-Things-you-need-to-do-if-your-Facebook-account-gets-hacked.html/
  - How a Friend's Hacked Facebook Account Can Compromise Your Privacy and Security http://facecrooks.com/Internet-Safety-Privacy/how-a-friends-hacked-facebook-account-can-compromise-your-privacy-and-security.html
  - Fake Facebook Profiles and Pages – the Tools of Scammers, Bullies and Thieves http://facecrooks.com/Scam-Watch/Fake-Facebook-Profiles-and-Pages-the-Tools-of-Scammers-Bullies-and-Thieves.html

Your Oxford username and passwords:

- If your Oxford email password or your single sign-on (SSO) has been given away contact IT Services, e.g. phishing@it.ox.ac.uk Do the same if you think someone else in the University has had their account hacked.

Licence

Hand-out: " do: social media security settings " by the Information Security team, University of Oxford, is licensed as Creative Commons Attribution-Non-Commercial-Share Alike 2.0 UK: England & Wales (http://creativecommons.org/licenses/by-nc-sa/2.0/uk/)