Protecting your Security and Privacy on the Web

Tony Brett

Head of IT Support Staff Services

IT Services

11 March 2013

Agenda

- Why bother?
- Common data leaks
- Email security
- Viruses & Trojans
- Phishing
  - Why you shouldn't click the link!
- Some common scams
- A note on paying for things
- Passwords are vital
  - Additional verification
  - 2 factor
- Cloud Services
  - Dropbox, Google Drive, Skydrive
  - Where is your data?
- Browser security
  - Cookies
  - Drive-by malware
- Social networking
  - They won't divulge what you don't tell them
  - Persistent web caches
  - Don't trust strangers too easily!
  - Facebook
- Twitter & Facebook Spam
- Wikis & Blogs
- Common Sense

Why bother?

- Your identity is valuable
- Identity fraud is rife!
- Access to your computer accounts can cause havoc for you and others
- Theft of your money
- Personal harassment
- Loss of data
- Loss of reputation
- Copyright breaches

Common data-leaks

- Bin raiding
- Impersonating deceased
- Insecure or Trojan websites
- Mail forwarding
- Phishing
- Skimming
- Theft of Wallet/Purse
- Unsolicited contact - scams

Email Security

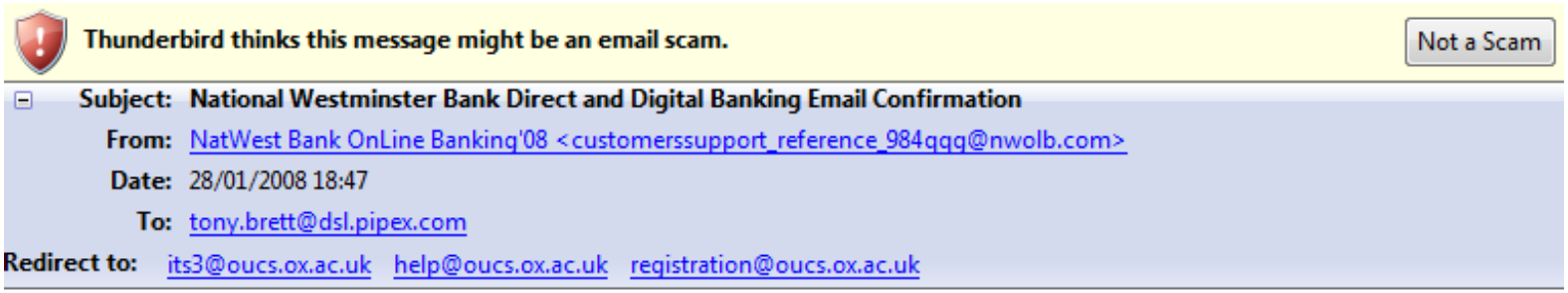
- Be careful of spam
  - Use a filter
- Vacation message should not say you are on holiday
- Don’t let others use your account
- Never open attachments you were not expecting
- Consider using digital encryption and signatures

Viruses and Trojans

- Viruses spread from PC to PC or via USB sticks
  - Can damage data
  - Can steal data
  - Can steal bandwidth
- Trojans may appear to be helpful
  - “Install this adware blocker for free...”
  - might be logging your keystrokes
  - DON’T install or run unknown things. Get advice!
- Beware “Scareware”
  - The call from “Microsoft” or the scary popup
- DO keep browsers up to date!
  - Most updates are security-related
- DO use anti-virus. KEEP IT UP TO DATE!
  - Sophos is free to University members
  - MS Security Essentials can be used on personal machines (but not work ones!)
  - Don’t forget your mobile device – Sophos now for Android too

Phishing

- Often tries to get online banking details or other logins such as your Oxford SSO
- May use a false link to entice you in to fake site
- NEVER follow links in email to online banking or password changing
- ALWAYS type the URL yourself or use a bookmark that YOU created
- Some mail programs and web browsers will spot phishing emails and sites
- Beware of giving any information extra to normal on a bank's site
- http://cups.cs.cmu.edu/antiphishing_phil/



NatWest

Dear Natwest Direct and Digital Banking user!

Our Maintenance Subdivision is performing a planned Online Banking software update

By following the link below please start the procedure of the user details confirmation:

http://www5.natwest.com/default.aspx?refid=24nhrtOfsdnnDleyOjzjdmOkhb

These directives are to be e-mailed and followed by all users of the NatWest Bank Direct Banking

NatWest Bank does apologize for the problems caused to you, and is very grateful for your collaboration.

If you are not user of Natwest Bank Digital Banking please disregard this notification!

=== This is robot generated message, please do not reply ===

http://www1.natwest.com.pas83.com/default.aspx?host=24nhrtOfsdnnDleyOjzjdmOkhb

But this is NOT Natwest!

More Phishing

- Phishers: why go for complex attacks when you can just ask for the password!

If you get emails from "Webmail account update Service Team" or any other similar-sounding body that asks you to supply your password then you MUST NOT REPLY to it. These emails are fake and are malicious attempts to gain access to your account. If you reply to such a message IT Services will have no choice but to disable your account for your own protection. Please JUST DELETE such messages. We will NEVER ask you for your password. EVER.

To All Department/Faculty,

Dear Webmail Subscribers ← They don't know who you are!

We hereby announce to you that your email account has exceeded its storage limit. You will be unable to send and receive mails and your email account will be deleted from our server. To avoid this problem, you are advised to verify your email account by Filling this Manual Information. This Message is From Help-desk. Due to our latest IP Security upgrades we have reason to believe that your webmail account was accessed by a third party. Protecting the security of your webmail account is our primary concern, we have limited access to sensitive webmail account features.

Failure to re-validate, your e-mail will be blocked in 24 hours. ← Threats – 3 times!

To avoid this problem,

You are advised to verify your email account for upgrading Now by clicking on the link

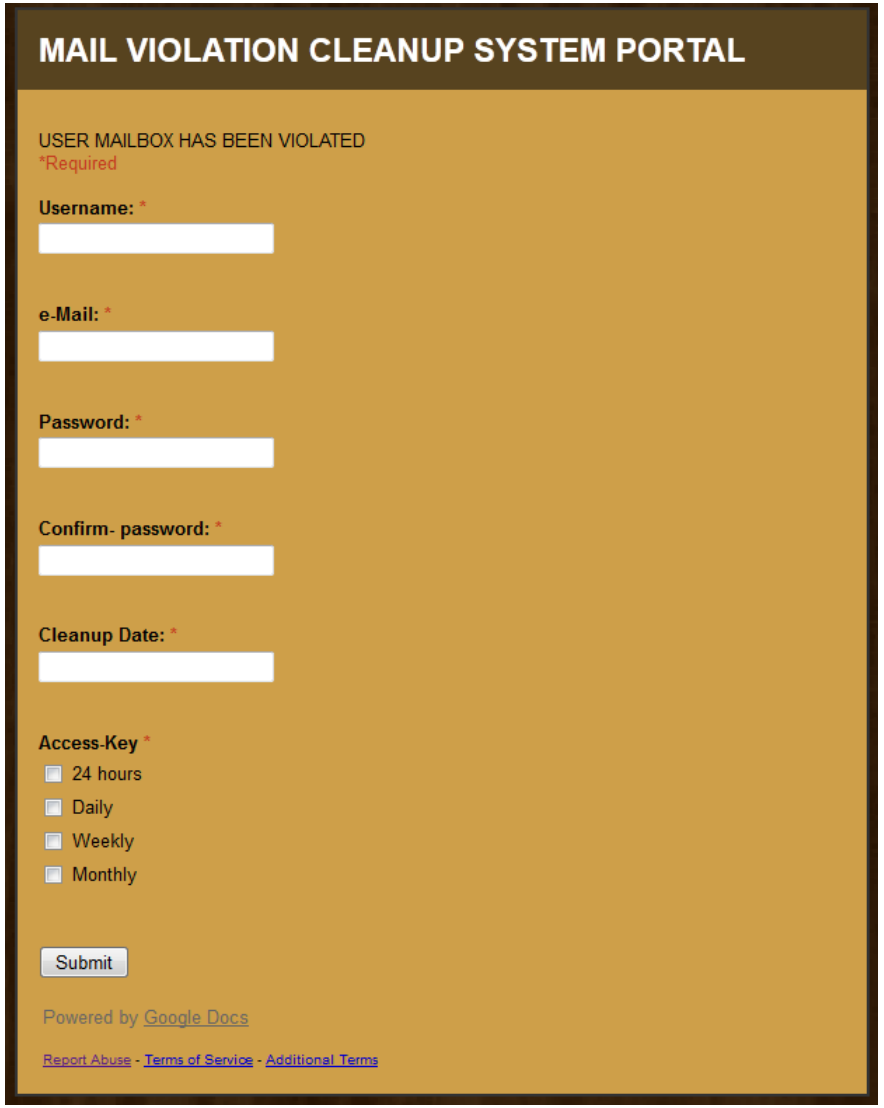
https://docs.google.com/a/hcc.edu/spreadsheet/viewform?formkey=dEZRSk1OQzhPNG9LUEZxb1c4UnFEZFE6MQ

Failure to do this will have your account deactivated to avoid unauthorized usage.

System Help Desk/Webmail Administrator

Don’t EVER fill in something like this

- If you do, please change your password quickly but also let IT Staff or IT Services helpdesk know without delay
- Also email phishing@it.ox.ac.uk



You've won the lottery!

- No you haven't...
  - You can't win it if you're not in it
  - In Russia they say:
  - "You get free cheese only in a rat trap"

We've identified you as only next of kin for...

- Also a fraud!
- Sometimes called the Nigerian or 419 Scam
- Sender tells you there is lots of money waiting for you
- But you have to send money by Western Union or similar first to cover "expenses"
- If you do it, problems start arising
  - Customs fees
  - Officials need bribing
- You never see any money!

The lesson...

- If it seems too good to be true...

IT ALMOST CERTAINLY IS!

A note on paying for things

- Always use a web seller with a phone number and real address
- Always pay by something secure e.g. paypal or credit card (less cover on debit card)
- Never pay by money transfer e.g. Western Union
- Be extremely suspicious if a trader asks you to pay by bank transfer (BACS)
- Only use BACS if you already have the goods and/or service.

Password advice

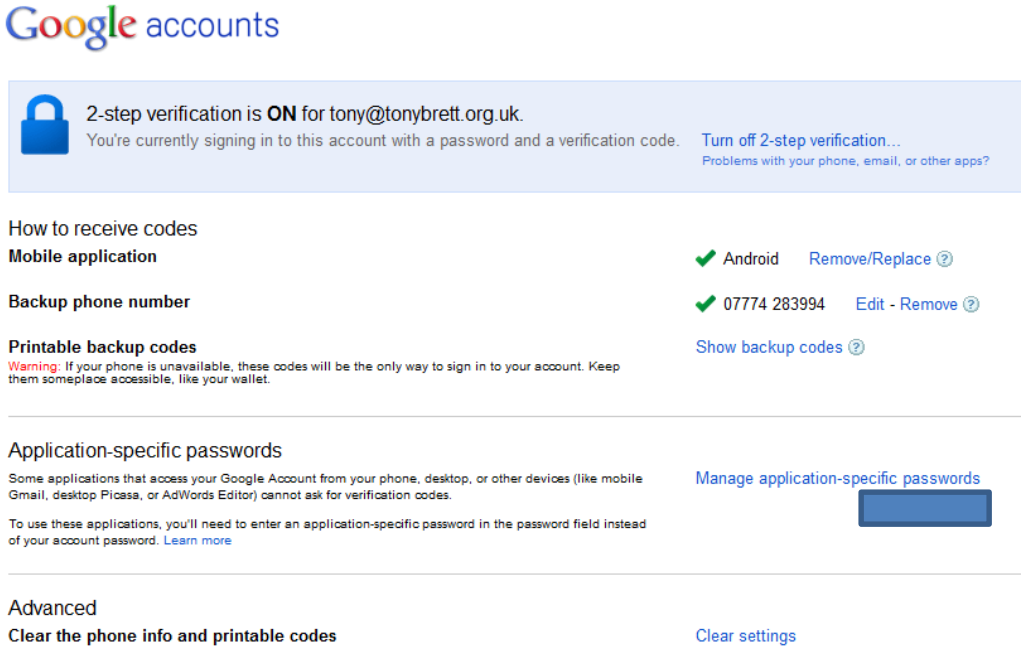
- 6-8 Characters or more
- Not based on a word
- Mixture of classes (= , A b ; + etc.)
- Do not give to ANYONE else
- Don’t stick a post-it of it under your keyboard
- Only write in a secure and unidentifiable form
- Use different passwords for different services
- Change regularly
- Think toothbrush!
- http://vimeo.com/3546084

How to remember so many passwords

- Consider something like KeePass
- User a strong master phrase and NEVER use it anywhere else

Additional Verification

- Available on Googlemail (called 2-step)
  - Sends a text to your mobile or uses a smartphone app



- Similar on other mail providers, facebook, dropbox etc.
- Use it!

What about “cloud” services

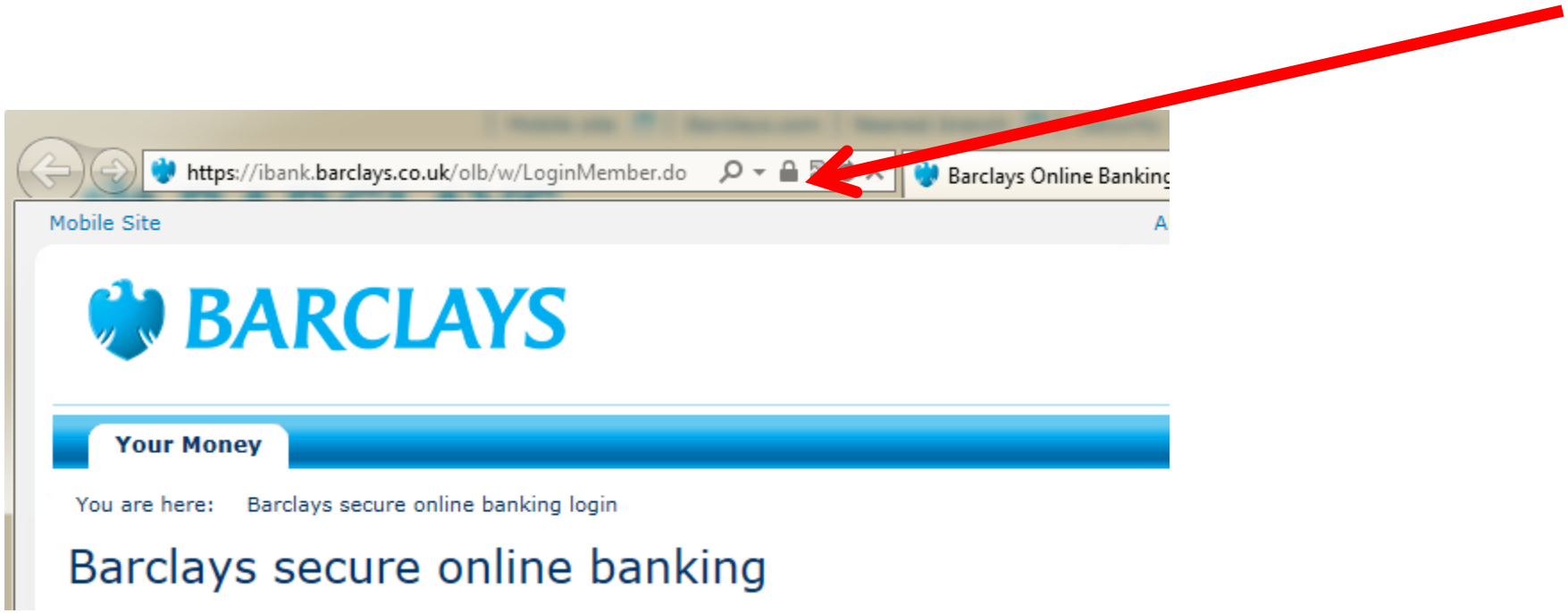
- Can be extremely useful and safe
- Think about what you are storing
- Especially useful with mobile devices (particuarly iPads and the like)
- Where is your data? D you know? Data Protection?
- Good, but not official Oxford, advice from http://www.unimelb.edu.au/infostrategy/policies/docs/dropbox.pdf
- Check the policy of your own College/department

Secure your Browser

- Make sure you can see the padlock before you put any personal details in
- Make sure the site is the site you think it is
- If in doubt don’t do it!
- Close your browser after doing secure online transactions

How to tell (Firefox)

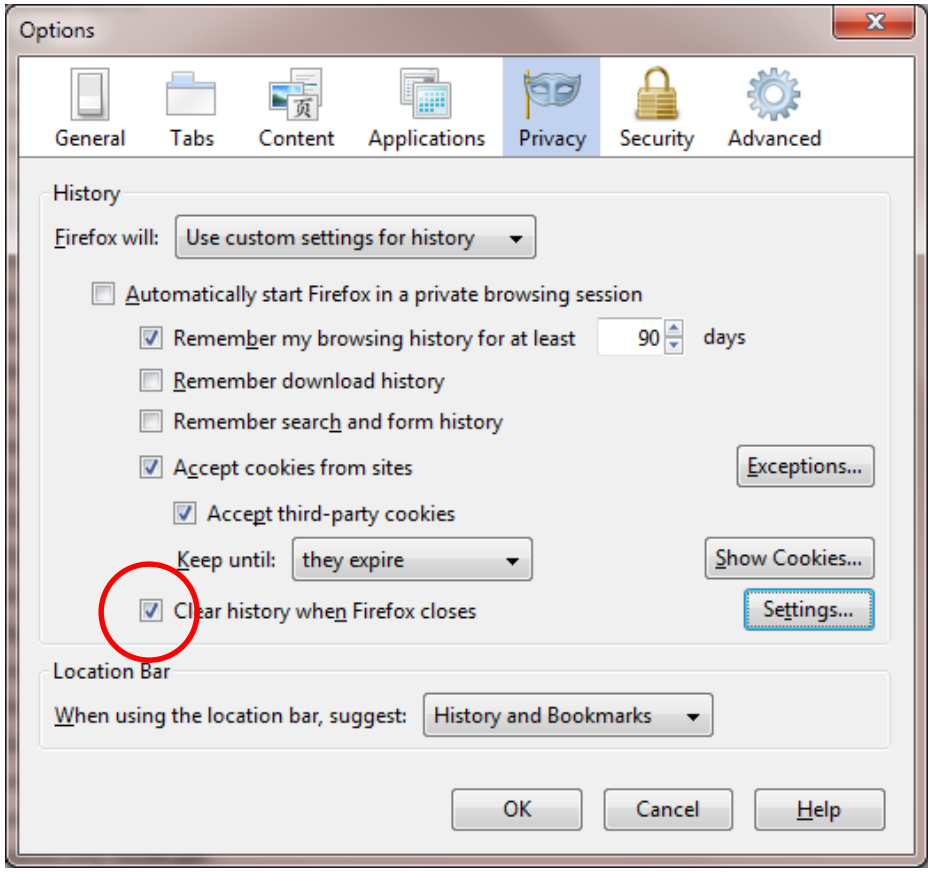
How to tell (Internet Explorer)

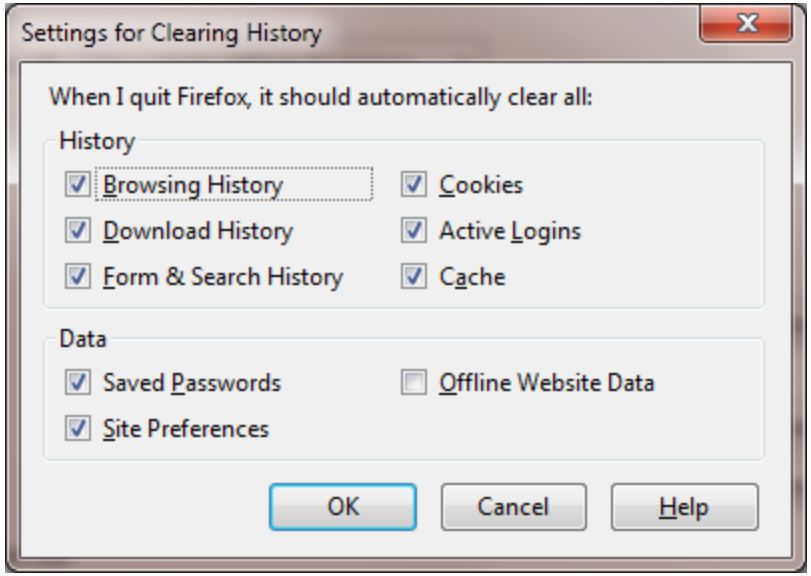


Cookies

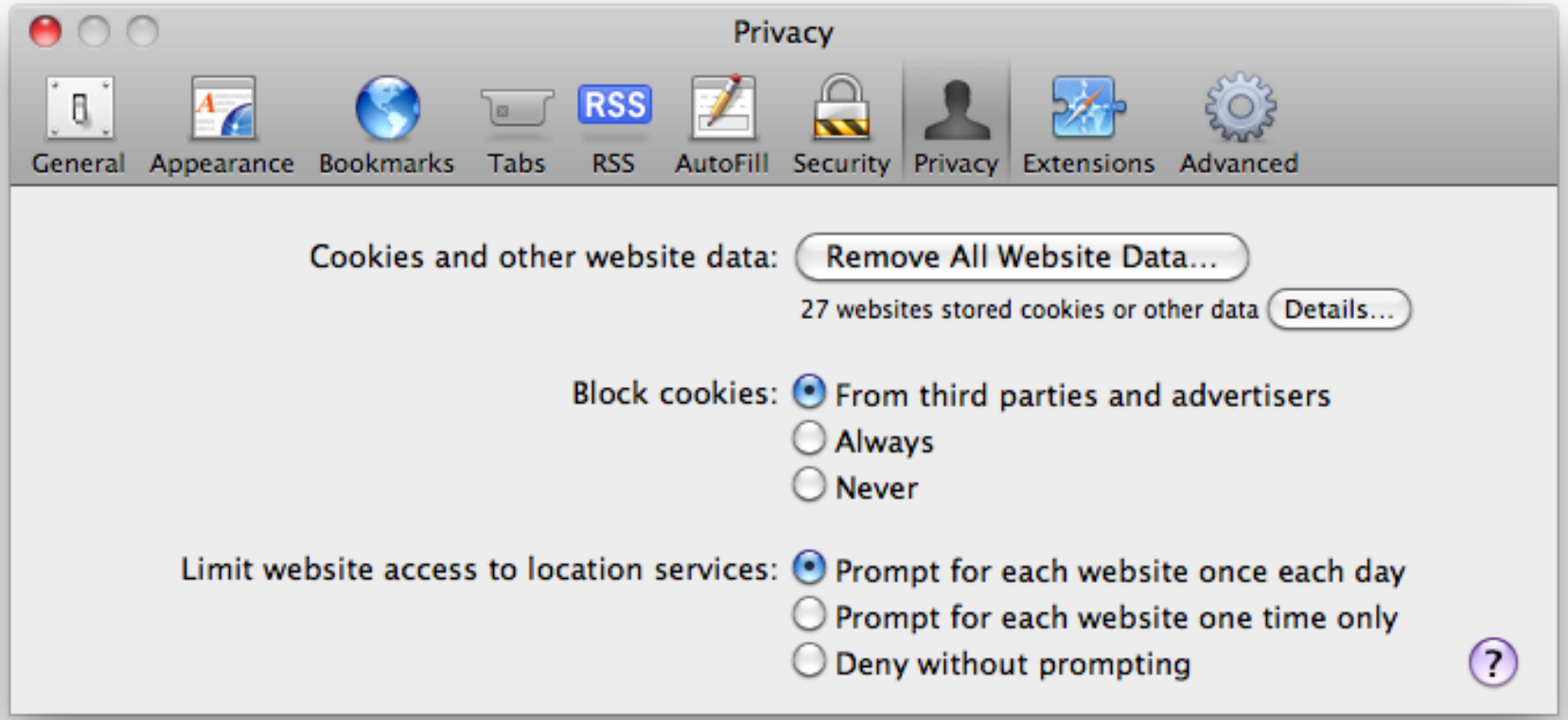
- Little bits of data that hold information about you and send them back to web sites
- Keep track of online transactions
- Set your browser to warn you about persistent cookies
- Session cookies generally OK and often essential
- You might not be as anonymous as you think!
- Deleting them all on exit is best security but does mean you have to re-type things.

Have Firefox auto-cleanup

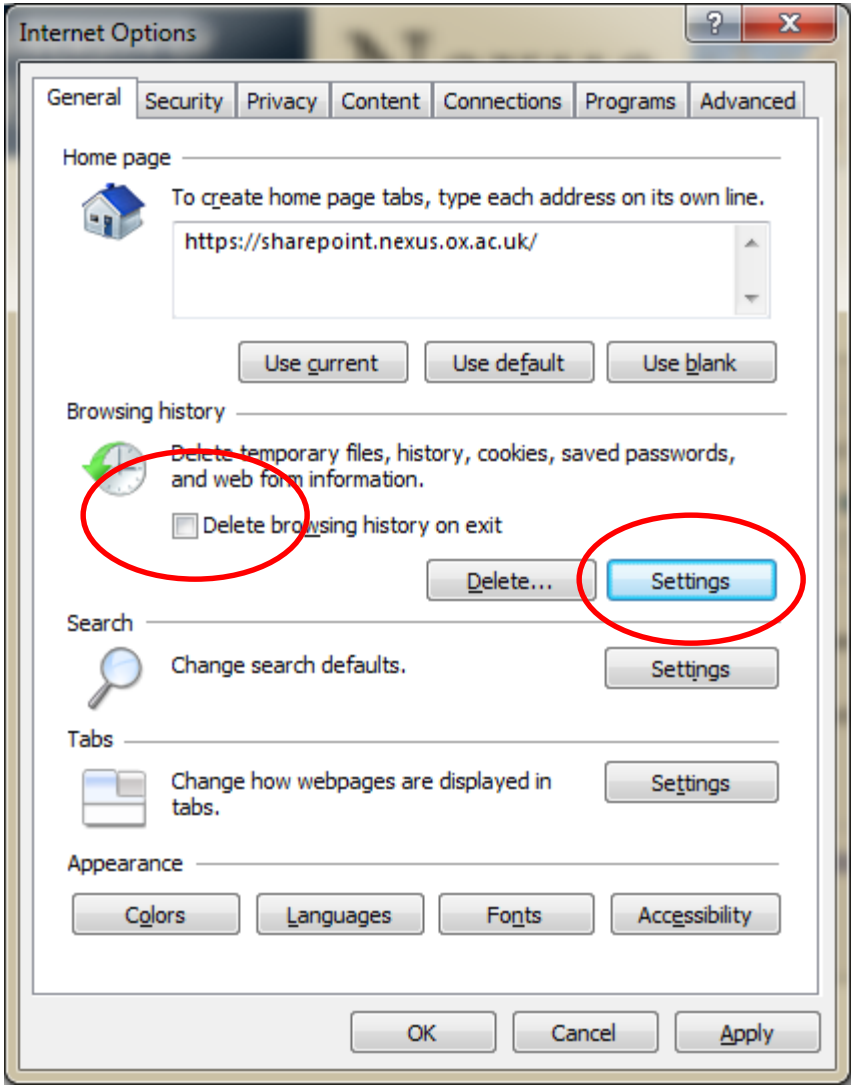


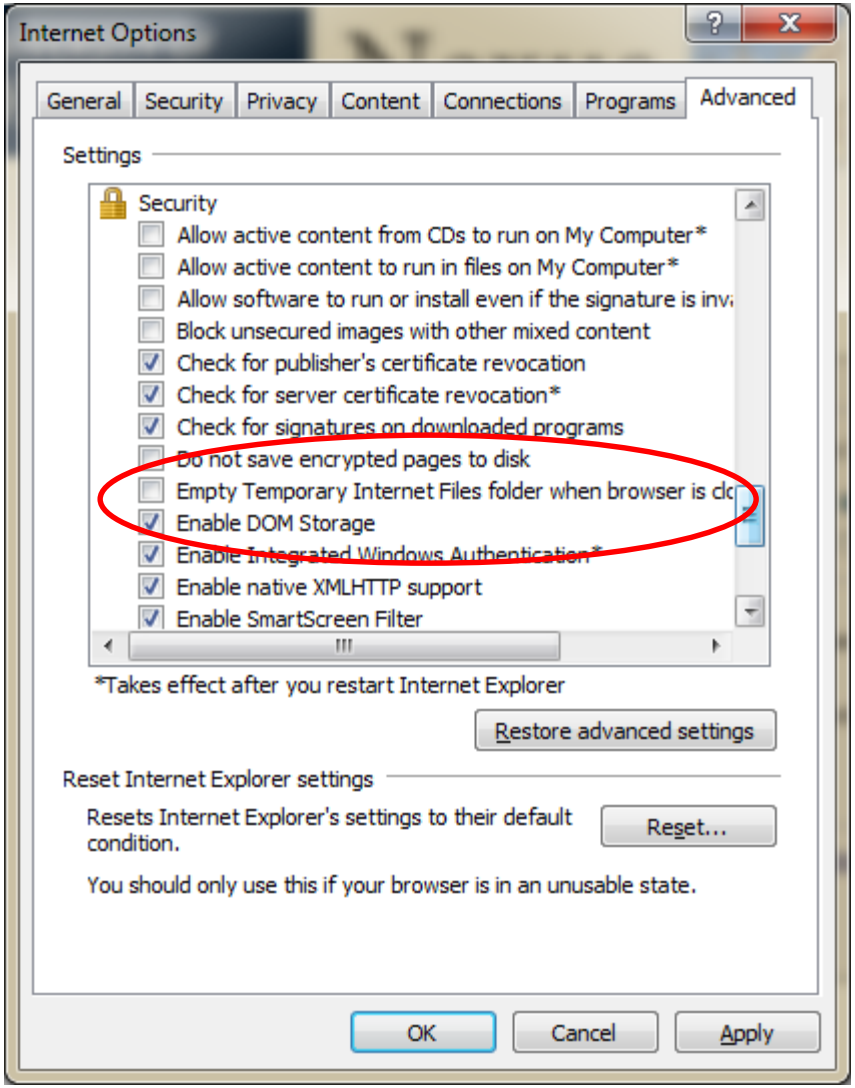


Have Safari auto-cleanup cookies



Clean up Internet Explorer





Popup Blockers & Ad Blockers

- Firefox and Internet Explorer can both block popups – use it!
- Some sites require popups so you can enable on a per-site basis
- Ad blockers are not standard
- Adblock Plus is really good in Firefox & Chrome

Social Networks – Facebook, LinkedIn etc.

- Great innovations
- Frameworks for many uses, not only social
- BUT can be a fraudster's paradise
- These sites can't reveal stuff you don't tell them
- Make sure privacy is set sensibly
- Be careful of random "friends" you don't actually know
- Learn how security and privacy works

General
Security
Privacy
Timeline and Tagging
Blocking
Notifications
Mobile
Followers
Apps
Adverts
Payments
Gifts
Support Dashboard

Privacy Settings and Tools

Who can see my stuff?	Who can see your future posts?	**Friends**	Edit
	Review all your posts and things you're tagged in		Use Activity Log
	Limit the audience for posts you've shared with friends of friends or Public?		Limit Past Posts
Who can look me up?	Who can look you up using the email address or phone number you provided?	**Friends of friends**	Edit
	Do you want other search engines to link to your Timeline?	**Off**	Edit

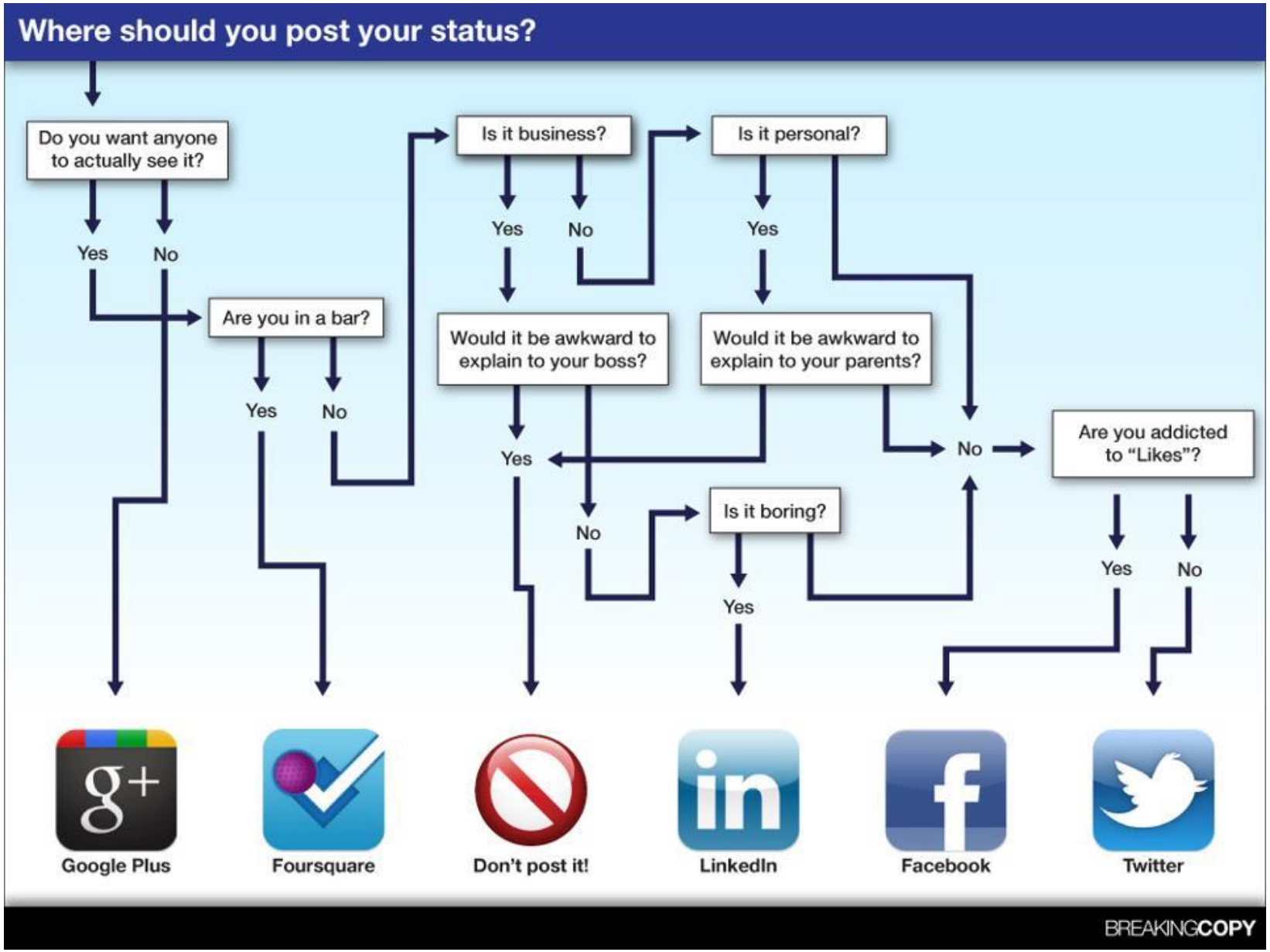
Timeline and Tagging Settings

Who can add things to my timeline?	Who can post on your timeline?	**Friends**	Edit
	Review posts friends tag you in before they appear on your timeline?	**Off**	Edit
Who can see things on my timeline?	Review what other people see on your timeline		View As
	Who can see posts you've been tagged in on your timeline?	**Friends**	Edit
	Who can see what others post on your timeline?	**Friends**	Edit
How can I manage tags people add and tagging suggestions?	Review tags people add to your own posts before the tags appear on Facebook?	**Off**	Edit
	When you're tagged in a post, who do you want to add to the audience if they aren't already in it?	**Friends**	Edit
	Who sees tag suggestions when photos that look like you are uploaded? (this is not yet available to you)	**Unavailable**	

Be careful what you show and say!

- Some things might embarrass you later
- You will be applying for jobs one day
- Be careful not to libel or defame others
  - Especially on Twitter
- Once things are online they are there for life
  - Even if you delete them there will be cached and archived versions
- My rule of thumb: Consider whether you'd want your mother to see it!

A handy (light hearted) guide!



Twitter & Facebook Spam & Phishing

- Watch out for new followers who are following lots of people but have few followers
- Watch out for links in tweets – you don't know where they go
- "Stranded in a foreign city" scams are becoming more common
  - know lots about you from your facebook friends
  - You never know who they are until you actually speak to them
  - Ring them back on a number they give you

Data is valuable

- Fraudsters can guess bank passcodes etc. If you give lots of info about yourself on social networking sites
- “Friends Reunited” can also provide useful information
- “… is 40 today” !!!
- Be careful with:

  DOB, NI number, mother’s maiden name, home address, previous address, employer, birthplace, school details

Wikis & Blogs

- Same rules apply
- Be careful about saying you're on holiday
  - (even just implying it with photos)
- Remember people can build up a profile of you to steal your ID

Common Sense

- If someone saying they are official rings you...
  - Have you verified them?
  - They would verify you if you rang them!
- Use good passwords
- Anti-Virus, Firewall, Anti-Spam
- Get a shredder
- Check your credit records with the agencies
  - Text alerts from banks and credit card companies are good
- Don’t leave dormant accounts lying around
  - They could be stolen without you knowing

Summary

- Be careful, suspicious and cynical
- Don’t trust people too easily
- Don’t do anything you are unsure about - ASK
- Ring people back on a number you look up
- Check identity if at all unsure
- Be careful what you say and share
- Challenge anything you are unclear about
- Be careful with links in emails
- Use strong and different passwords and change them regularly – consider a password manager
- Keep your antivirus and web browsers up to date

Questions?

References

- http://users.ox.ac.uk/~tony/websecurity.pdf
- http://adblockplus.org
- http://www.stop-idfraud.co.uk/
- http://www.cardiff.ac.uk/insrv/it/help/safe/security.html
- https://register.oucs.ox.ac.uk/software
- http://www.microsoft.com/en-us/security_essentials/default.aspx
- http://keepass.info/
- http://cups.cs.cmu.edu/antiphishing_phil/
- http://www.ictf.ox.ac.uk/conference/2009/presentations/cluley.pdf
- http://www.sophos.com/blogs/gc/
- http://vimeo.com/3546084
- http://www.unimelb.edu.au/infostrategy/policies/docs/dropbox.pdf
- http://www.sophos.com/en-us/products/free-tools/sophos-mobile-security-free-edition.aspx