



Police Training – Cybercrime & Prevention Train the Trainer Session Notes

In these notes

- ◆ Introductions
- ◆ Terminology
- ◆ The law
- ◆ The basics
- ◆ The Get Safe Online website
- ◆ Specific risks/threats

The screenshot shows the homepage of the Get Safe Online website. At the top, there is a navigation bar with the logo 'GET SAFE ONLINE' and the tagline 'Get Safe Online Free expert advice'. Below this, there are tabs for 'Personal' and 'Business'. The main content area features several articles and sections:

- Protecting Your Computer**, **Protecting Yourself**, **Smartphones & Tablets**, **Shopping, Banking & Payments**, **Safeguarding Children**, **Social Networking**, and **Business**.
- A large article titled "Figures from TalkTalk show extent of scam phone calls" with a photo of a man on a phone.
- Other articles include "Over £1bn lost by businesses to online crime in a year", "#RedCardCrime tackles online ticket fraud", "Fake 'WhatsApp Gold' link results in malware", and "Millions of LinkedIn passwords and email addresses for sale".
- A section titled "Get the answers" with a question: "Do you have a question about online safety?" and a link to "Ask Terry Tablet".
- A section titled "Can your business afford not to take online safety & security seriously?" with a photo of a woman at a computer.
- A "Tweets" section featuring a tweet from @YH_CyberProtect and a link to a video titled "Policing YORKSHIRE & THE HUMBER".
- A section titled "Don't become prey for a fraudster" with the text "Think twice BEFORE YOU ACT".
- A section titled "New to the internet?" with the text "We'll help you use it with safety and confidence. Start by reading our top ten tips." and a link to "Click Here".
- A section titled "What to watch out for Current scams" with a warning icon and the word "phishing".
- A section titled "Watch our great advice videos" with a link to "Click Here".

At the bottom, there is a footer with logos for various partners including PCC, TESCO, NatWest, and KASPERSKY.



Using the internet

What do you do online?

- ✦ Shopping?
- ✦ Booking holidays?
- ✦ email?
- ✦ Searching?
- ✦ Staying in touch?
- ✦ Social media?
- ✦ Music / films?
- ✦ Dating?



What's at stake if something goes wrong?

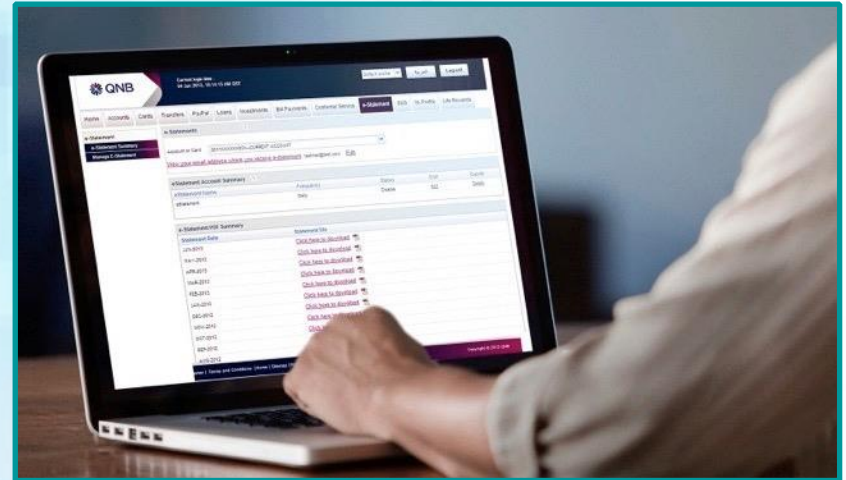
- ◆ Financial loss
- ◆ Time
- ◆ Credit rating
- ◆ Sanity/health
- ◆ Reputation
- ◆ Personal safety



Terminology (Hardware)

Essentially, these are all types of computer

- ◆ Computer
- ◆ PC
- ◆ Mac
- ◆ Laptop
- ◆ Tablet (iPad, Hudl etc)
- ◆ Smartphone
- ◆ Gaming console



Terminology (Software)

- ◆ Computer program
- ◆ Software
- ◆ Code
- ◆ Script
- ◆ Application (App)
- ◆ Browser
- ◆ Search engine
- ◆ Antivirus
- ◆ Firewall



Terminology (People)

- ◆ Computer programmers
- ◆ Coders
- ◆ Developers
- ◆ Software engineers
- ◆ IT support personnel
- ◆ Information assurance personnel
- ◆ **FRAUDSTERS!**



Terminology (Malware) malicious software

- ✦ Virus
- ✦ Trojan (Trojan horse)
- ✦ Worm
- ✦ Spyware
- ✦ Adware
- ✦ Ransomware
- ✦ Scareware
- ✦ Blended threat



Terminology (Cybersecurity)

- ◆ Internet Security
- ◆ Online Safety
- ◆ Computer Security
- ◆ Network Security
- ◆ Information Security
- ◆ Information Assurance
- ◆ IT Security
- ◆ Data Protection



Terminology (Cybercrime)

Cyber enabled crime:

Crimes that may be committed without IT devices, but are changed significantly by the use of it in terms of scale and reach

Cyber dependent crime:

Crimes that can be committed only through the use of IT devices, where both the tool for committing the crime and the target of the crime is an IT device

Internet facilitated crime:

Crimes that involve the use of the internet to facilitate drug dealing, people smuggling and many other 'traditional' crimes

Relevant laws include:

- ◆ Computer Misuse Act 1990
- ◆ Data Protection Act 1998
- ◆ Copyright Designs & Patents Act 1988
- ◆ Protection from Harassment Act 1997
- ◆ Grooming: Sexual Offences Act 2003 S15
- ◆ Blackmail: Theft Act 1968
- ◆ Indecent Images of Children:
The Protection of Children Act 1978
- ◆ Fraud Act 2006



The basics

...you need to follow three basic 'rules'

- ✦ Choose, use and protect your passwords carefully
- ✦ Ensure that you have internet security software / app that is always kept up to date and switched on
- ✦ Update your operating system and all other software as soon as prompted

It is estimated that if everyone followed these steps, 80% of cybercrime would be prevented



Get Safe Online website

- ◆ Easy to use
- ◆ Simple language
- ◆ Comprehensive
- ◆ UK Government backed
- ◆ Impartial
- ◆ Free to use
- ◆ Personal & Business sections
- ◆ Google Search and Virtual Assistant
- ◆ Short educational videos

The screenshot shows the homepage of the Get Safe Online website. At the top, there is a navigation bar with links for Home, About Us, Partners and Supporters, Press, News, Blog, Jason Buster, and Contact. Below this is a search bar and social media icons. The main content area is divided into sections: Personal and Business. The Personal section includes links for Protecting Your Computer, Protecting Yourself, Smartphones & Tablets, Shopping, Banking & Payments, Safeguarding Children, Social Networking, and Business. The Business section includes links for Protecting Your Computer, Protecting Yourself, Smartphones & Tablets, Shopping, Banking & Payments, Safeguarding Children, Social Networking, and Business. The main content area features a large image of Commander Chris Greany, the new chair of Get Safe Online, with a caption. Below this are several featured articles and videos, including 'Whatever kind of break you're planning this year - make sure it's one that really exists', 'Don't become prey for a fraudster', 'New to the internet?', 'What to watch out for Current scams', and 'Watch our great advice videos'. The footer contains logos for partner organizations: TESCO, LLOYD'S BANK, HALIFAX, NatWest, KASPERSKY, and BARCLAYS.



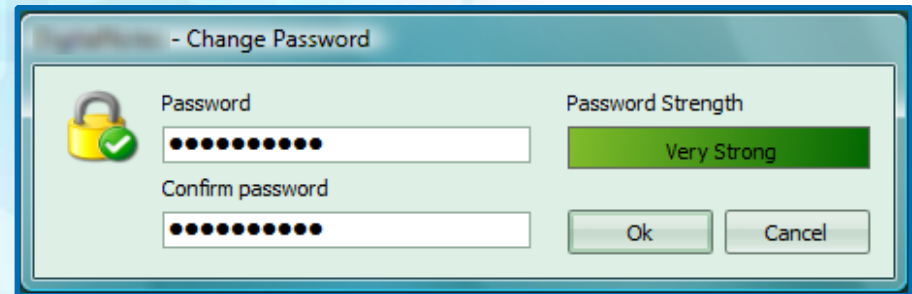
Website (New to the internet)

- ◆ Passwords/PINs
- ◆ Internet security software
- ◆ Mobile devices
- ◆ Wi-Fi hotspots
- ◆ Protecting your personal information
- ◆ Masqueraders and impersonators
- ◆ emails, links & attachments
- ◆ Direct bank transfers
- ◆ Think twice, click once
- ◆ If it seems too good to be true...



Passwords - basics

- ◆ Always use a password
- ◆ Ensure you use strong passwords, and do not disclose them to *anyone* else
- ◆ Don't use easy-to-guess passwords
- ◆ Use PINs on all mobile devices



Passwords - Why they really matter

- ✦ Authorisation = are you allowed to do this?
- ✦ Authentication = who are you?
- ✦ Passwords simply provide authentication, ie proving your ID



Passwords - Creating, storing and remembering

- ◆ Size matters, minimum 8 characters
- ◆ Alphanumeric
- ◆ UPPER and lower case
- ◆ Keyboard characters
- ◆ Use different passwords for different accounts
- ◆ How do you remember them without compromising them?
 - ◆ Write them down in code eg H0me5555 = XXxxSSSS
 - ◆ Consider using a Password Vault on your smartphone/tablet



Internet Security Software

An all-in-one internet security package is normally more than adequate.

- ◆ Microsoft Security essentials (free on PCs)
- ◆ AVG
- ◆ Avast
- ◆ Norton
- ◆ McAfee
- ◆ Kaspersky
- ◆ Trend
- ◆ F-Secure
- ◆ ESET
- ◆ BitDefender

Typical cost £30.00.

Some also offer free versions



Internet Security Software

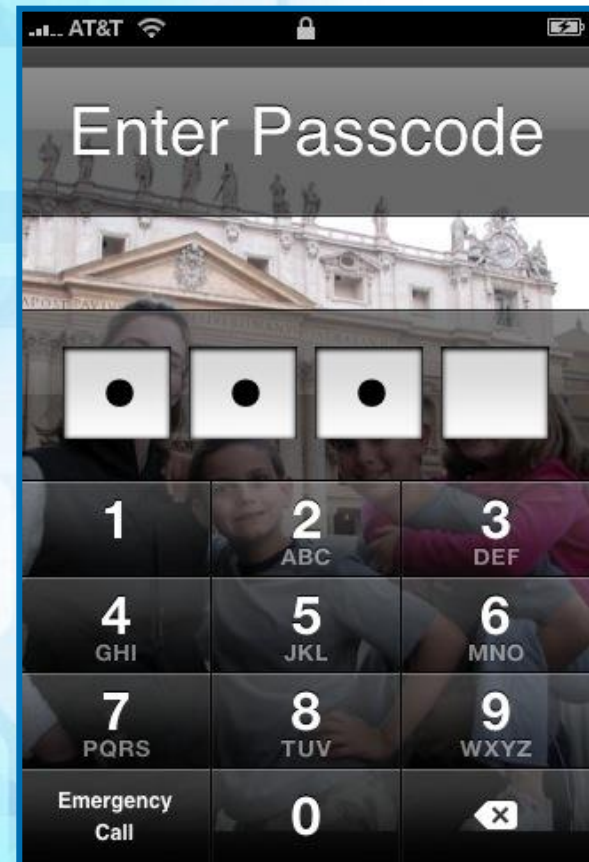
An all-in-one internet security package will contain many of the following:

- ✦ Antivirus/antispyware
- ✦ Firewall
- ✦ Real time scanning
- ✦ Website advisory tools
- ✦ Parental controls
- ✦ Privacy protection
- ✦ Wi-Fi protection
- ✦ File deletion tools
- ✦ PC optimisation
- ✦ Device location and/or remote disabling (mobile security apps)



Mobile devices

- ◆ Risk of loss or theft
- ◆ Risk of damage
- ◆ Risk of going down the toilet!
- ◆ Easy access to all apps
- ◆ Put a PIN on it



WiFi Hotspots

- ◆ Assume they are insecure, they probably are
- ◆ It's also easy to set up a fake mobile hotspot
- ◆ Use 3G or 4G, a Virtual Private Network (VPN) or secure mobile dongle
- ◆ Coffee shops sell coffee ... not security



Too much information!

- ◆ Be careful about the personal information you disclose, remember it can all be pieced together to clone your identity
- ◆ Privacy is not about having something to hide; it is about having the right to control what you want to share and what you want to keep to yourself



Masqueraders and impersonators

- ◆ The great thing about the internet is nobody knows you're a dog (but you don't know if the person you're dealing with is a dog either)
- ◆ Ensure you verify people's identity, both on the internet and phone calls



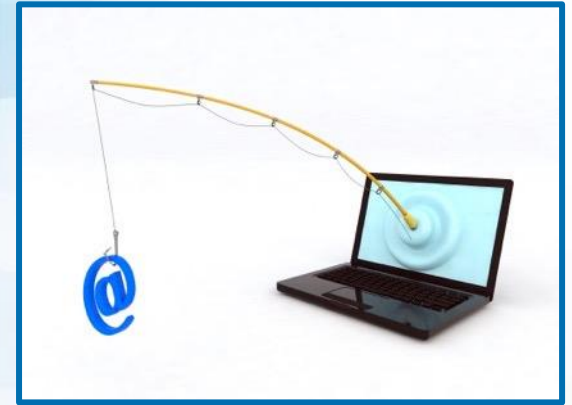
email

- ✦ One of the most common things we all use
- ✦ There are many security issues associated with email
- ✦ The fraudster's favourite



Email

- ◆ Having access to your email is like having the keys to the kingdom
- ◆ Forgotten passwords
- ◆ Where you shop (receipts)
- ◆ Access to your friends/contacts
- ◆ It's easy to masquerade as you
- ◆ Malware (in attachments and links)
- ◆ Phishing (emails that are trying to get your personal details)
- ◆ Fraud scams (HMRC, parcel delivery firms, Apple are amongst the most commonplace)




Spam and Scam email

- ◆ Always be vigilant when receiving or responding to emails
- ◆ Make sure your spam filter is always switched on to minimise the risks



Phishing (Example email)

 **Nationwide** proud to be different

Dear Customer,

Nationwide's Internet Banking, is here by announcing the New Security Upgrade. We've upgraded our new SSL servers to serve our customers for a better and secure banking service, against any fraudulent activities. Due to this recent upgrade, you are requested to update your account information by following the reference below.

<http://www.nationwide.co.uk/update.asp?ID=3b89db2a6001ec93328d21e59a011b0a25a>

<http://www.drinkrezepte.de/shakes/index.html>

Regards

Rafiq Miah

Customer Advisor

Nationwide Direct

Nationwide Building Society

email

DO YOU ...

- ✦ Assume an email is genuine and look for clues to suggest it's fake?

OR

- ✦ Assume an email is fake and look for clues to suggest it's genuine?

Check the context, ie is a family member addressing you as '*Dear friend*', or a company whom you have an account with as '*Dear customer*'?

Making payments and transferring money

- ✦ Use recognised payment methods (PayPal, Worldpay)
- ✦ Credit card payments offer the most protection
- ✦ Never transfer money to another's bank account
- ✦ Scammers will often ask you to make direct bank transfers due to a 'problem with the normal payment method'
- ✦ Once money is transferred, it's normally unrecoverable and not refundable by the bank



Think twice, click once

Slow down, don't be pressured

Always double check:

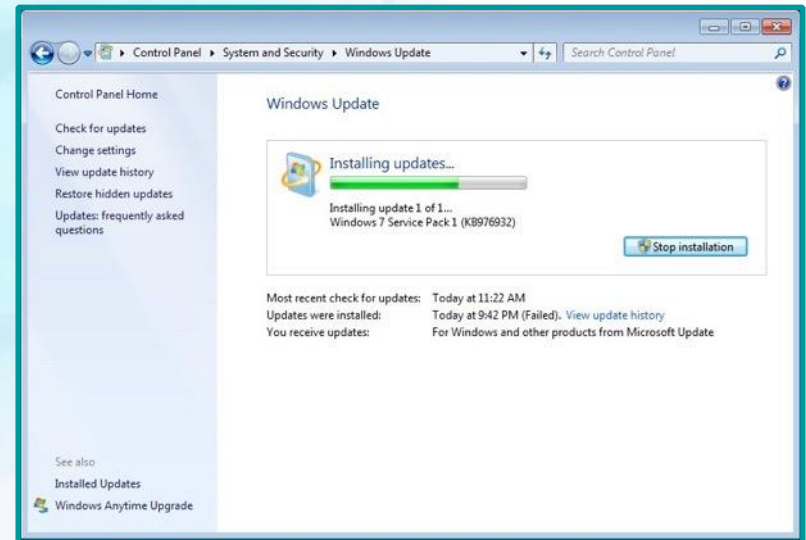
- ✦ That websites are genuine
- ✦ Payment details
- ✦ Identities of officials, and callers
- ✦ email addresses



And if something seems too good to be true, it probably is!

Windows and other software updates

- ✦ Download and install Windows updates as soon as possible after being alerted that they are available
- ✦ These updates also contain security improvements and new functions
- ✦ Check these are genuine before installing.
- ✦ Set to automatically update where possible



Malware (Viruses & Spyware)

- ◆ An all-in-one internet security package will contain antivirus and antispyware tools, scan your device and even locate / disable your mobile device
- ◆ Some include parental software
- ◆ Some cover multiple devices



Malware (Ransomware)

Cryptolocker 2.0

Your personal files are encrypted



Your files will be lost
without payment on:

11/24/2013 3:16:34 PM

Info

Your **important files were encrypted** on this computer: photos, videos, documents, etc. You can verify this by click on see files and try to open them.

Encryption was produced using **unique** public key **RSA-4096** generated for this computer. To decrypt files, you need to obtain **private** key.

The single copy of the private key, which will allow you to decrypt the files, is located on a secret server on the Internet; **the server will destroy the key within 72 hours after encryption completed**. After that, nobody and never will be able to restore files.

To retrieve the private key, you need to pay 0.5 bitcoins.

Click **proceed to payment** to obtain private key.

Any attempt to remove or damage this software will lead to immediate private key destruction by server.

See files

<< Back

Proceed to payment >>



'Webcam blackmail' (Sextortion)

- ✦ Sexual exploitation by means of coercion
- ✦ Never get lured into removing your clothes or performing sexual acts in front of your webcam
- ✦ If victimised, do not pay any fees but report the crime, however embarrassing it may seem at the time



ABOUT YOUR VIDEO
I CAN EASILY DELETE IT IF I
WANT, BUT YOU NEED TO
PAY ME

Online radicalisation

- ◆ Be wary of attempts to radicalise you or those you know, and consider the consequences to yourself, family and friends
- ◆ Report attempted or actual radicalisation immediately by clicking the red button on Get Safe Online and other websites



Device disposal

- ✦ Deleting files and other content from computers and mobile devices does not generally actually delete the data
- ✦ This data may not have been properly erased and can be retrieved by criminals with the minimum of effort
- ✦ Ensure data is properly deleted, or destroy the device



Physical security

- ◆ Make sure your computers and mobile devices are protected against theft, flood, fire and accidental damage
- ◆ Protect computers and mobile devices against data loss and unauthorised access
- ◆ Remember that the convenience of your mobile devices also means they are very easy to lose and for criminals to steal
- ◆ Don't leave devices unattended, or in vehicles, even if locked



Physical Security

- ◆ Shoulder surfing – be aware of who's around and behind you, watching your screen
- ◆ Eavesdropping – quoting your personal details, logins, card numbers in public places can lead to trouble



Backups

- ✦ Ensure that all your important data is backed up regularly to a secure place
- ✦ Ensure that your backed up data will always be retrievable when you need it



There are many ways to back everything up:

- ✦ *Cloud (like OneDrive, iCloud, DropBox)*
- ✦ *External hard drive*
- ✦ *USB stick*

*Make sure where you back it up to a safe, memorable place.
Some are cheap, some are free!*

Backups

- ◆ External hard drives
 - 1 Terabyte (1TB) £47.00
 - 2 Terabyte (2TB) £60.00
- ◆ Cloud
 - Lots of benefits and can be free



Safe internet use

- ◆ www - stands for World Wide Web, but could also mean Wild Wild West!
- ◆ Always be vigilant when supplying personal or financial details
- ◆ Type the address in carefully, don't click on links in emails, texts or social media



Safe internet use

- ◆ Ensure your browser is the latest version.
- ◆ Make sure it is up to date
- ◆ Green padlock in the address line
- ◆ https://: ('s' stand for 'secure')



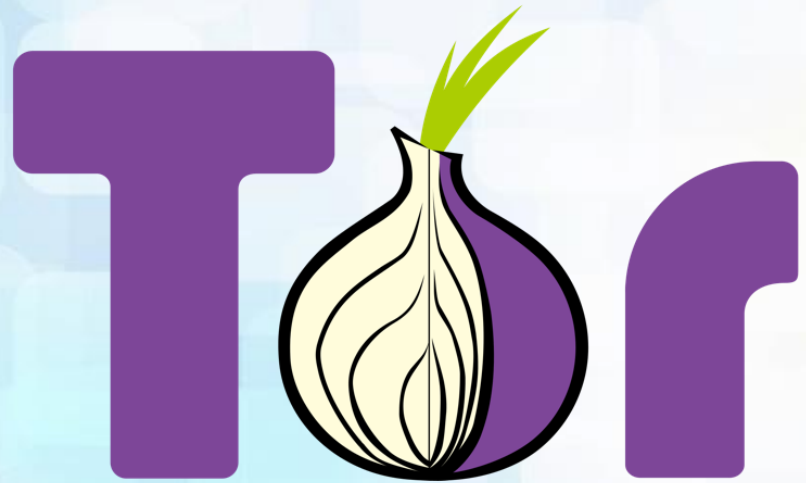
Safe internet use

- ✦ Your logon to most sites is normally your email address. Therefore different passwords for each site is very important as if one account gets hacked, your others are at risk
- ✦ Remember: if an account is compromised it will take at least an hour or two to fix. Imagine if all your accounts were compromised.



Safe internet use

- ✦ TOR (The Onion Router)
- ✦ Offers anonymity on the internet
- ✦ Has honourable uses, but also a haven for criminals (drugs, arms, stolen data, child abuse, extremist & hate content)



Simple encryption (Caesar Cipher)

Plain text

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z _

_ A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Cipher text

Key is 'one to the right'

the eagle has landed

sgdzd fkdzg rzk mcdc

Simple encryption (Caesar Cipher)

Plain text

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z _

_ A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Cipher text

Key is 'one to the right'

HZKNUDZXNTZQNA

Enigma machine

- ◆ 158,000,000,000,000,000,000 ways to set up
- ◆ Therefore, code was unbreakable, or so it was thought



Shopping

- ◆ Choose reputable, genuine shopping sites
- ◆ Ensure the payment page is secure before entering payment details
- ◆ Check reviews, and if something is very cheap there's normally a reason



Banking

- ◆ Beware of phishing emails that request you to enter login details on a website
- ◆ Beware of vishing phone calls that ask you to reveal your login details to overcome a 'problem' with your account
- ◆ Use strong passwords and keep them secure

A screenshot of a web-based "Change Password" dialog box. It features two password input fields, one for the current password and one for the new password, both masked with dots. To the left of the first field is a yellow padlock icon with a green checkmark. To the right is a "Password Strength" indicator showing a green bar and the text "Very Strong". At the bottom right are "Ok" and "Cancel" buttons.

Social engineering

- ✦ Always be wary of people requesting confidential or personal information by whatever means, however convincing they may seem
- ✦ As hacking has become more difficult, it is much easier to ask for someone's logon details
- ✦ There are a lot of variations of social engineering



Don't become prey for a fraudster

Think twice
BEFORE YOU ACT



Telephone banking fraud

- ◆ If you're called by someone claiming to be your bank requesting confidential details, call your bank on what you know is the correct number but wait five minutes or call a friend first.
- ◆ Banks, police, HMRC & other organisations do *not* call & ask for confidential information
- ◆ Treat any cold call with extreme caution. Always double check



Wait 5 minutes
OR
Phone a friend



Mobile banking

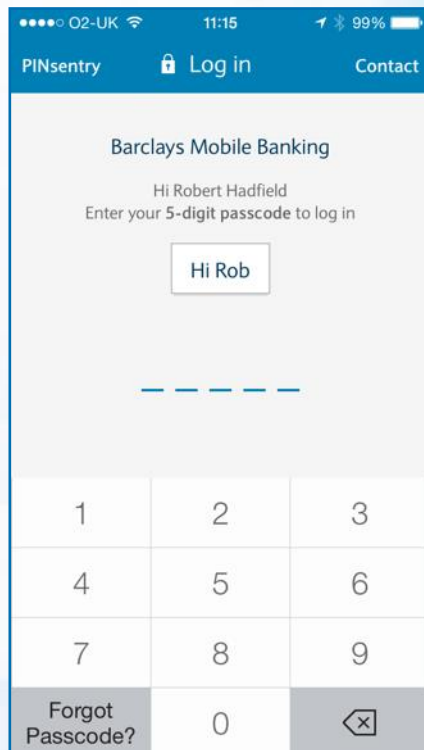
- ✦ Use only banking apps from authorised app stores, and make sure mobile banking sites are authentic and secure
- ✦ Use only Wi-Fi you know to be secure, eg at home/office or 3G/4G when doing mobile or any online banking or other financial transactions
- ✦ As with any online banking, choose and use strong passwords and keep them to yourself



Mobile v. online banking

Mobile App

Laptop



Mobile v. online banking

Lots of Browsers - Lots of versionsApp



IE 11

Firefox 48

Chrome 51

Safari 9

Opera 37

Pension fraud

- ◆ Be wary of any approaches by phone, email, text or in person about cashing in your pension before you reach retirement age
- ◆ Be wary of approaches to invest your lump sum ... especially those with returns that seem too good to be true (because they probably are)
- ◆ Always speak to a financial adviser who is registered with the Financial Conduct Authority



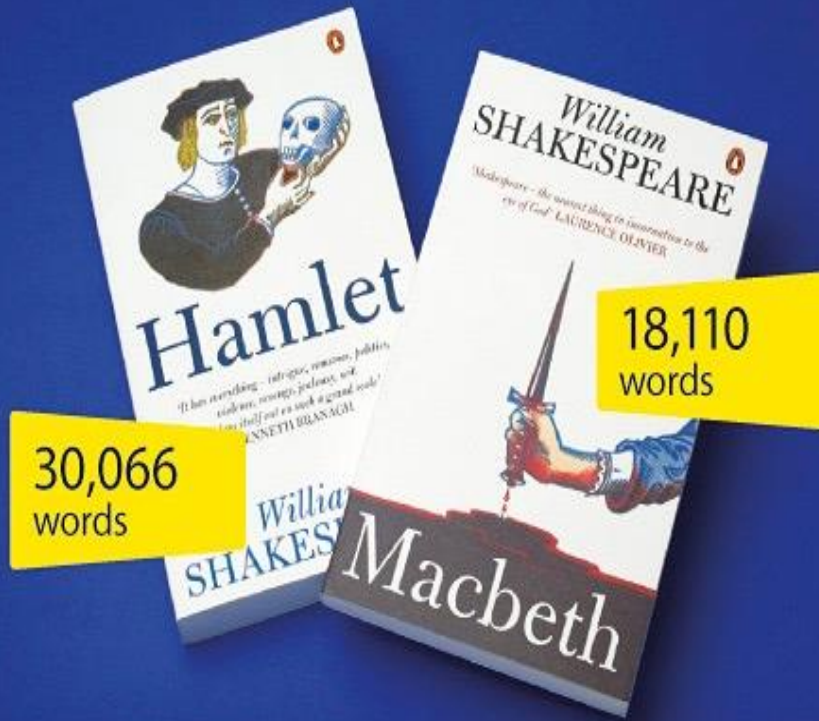
Accepting terms & conditions

- ✦ Read terms & conditions before accepting them
- ✦ This seems pretty obvious but it's not that easy (usually very long and complex)



Accepting terms & conditions

Which?



WEBSITE/SERVICE/BOOK	TOTAL WORDS*
PAYPAL	36,275
HAMLET	30,066
APPLE ITUNES	19,972
MACBETH	18,110
WINDOWS LIVE	14,714
APPLE iOS 5	13,366
FACEBOOK	11,195
GOOGLE ALL-INCLUSIVE	10,640
APPLE ICLOUD	10,724
AMAZON KINDLE	7,115
AMAZON.CO.UK	5,212
TWITTER	4,445
GOOGLE	4,099

Accepting terms & conditions

Specifically for photos and video uploaded to the site, Facebook has a license to use your content in **any way it sees fit**, with a license that goes beyond merely covering the operation of the service in its current form. Facebook can **transfer** or **sub-license** its rights over a user's content to another company or organisation if needed. Facebook's license does not end upon the deactivation or deletion of a user's account, content is only released from this license once all other users that have interacted with the content have also broken their ties with it (for example, a photo or video shared or tagged with a group of friends)

Subscription traps

- ◆ Beware of offers that seem too good to be true
- ◆ No one is really selling iPhones for £1
- ◆ Also commonplace for 'free' or 'low cost' trials of slimming pills & beauty products
- ◆ Read the small print
- ◆ Strictly speaking, these are misleading rather than illegal, but can be impossible to get out of



General advice

- ◆ If in doubt, get a second opinion, phone a friend
- ◆ Check things out directly with the organisation concerned
- ◆ Scammers normally increase pressure/urgency to lure you in
- ◆ Use Google, YouTube, Wikipedia etc to learn more
- ◆ Enjoy the internet



Further help and advice

✦ www.getsafeonline.org



www.getsafeonline.org

✦ Internet Watch Foundation
www.iwf.org.uk



✦ www.ceop.police.uk



✦ www.victimsupport.org.uk



www.getsafeonline.org



And don't forget...

- ✦ Don't think "it will never happen to me"
- ✦ Don't get into bad habits
- ✦ Don't take online safety for granted
- ✦ Don't do anything online that you wouldn't do offline
- ✦ Think twice
- ✦ Check out www.getsafeonline.org for further expert, free information & advice

The screenshot shows the homepage of the Get Safe Online website. At the top, there is a navigation bar with links for Home, About Us, Partners and Supporters, Get Behind Us, Press, News, Blog, James Butler, and Contact. Below this is a search bar and social media icons for Facebook and Twitter. The main content area features several sections: a large banner for 'national savings & investments' with the NS&I logo and a warning about a 'Fake National Savings website targets pensioners'; a 'Get the answers' section with a question about online safety; a 'BBC Crimewatch is working with Get Safe Online against Revenge Porn' section; a 'Tweets' section with recent posts from @GetSafeOnline; and a footer with logos for BBC, HM Government, Action Fraud, PayPal, NCA, Ofcom, and Norton.

