u3a Computing Group

Alan Hopwood, 4 April 2024

Agenda

Welcome
Current News, Issues and Questions
Topic list
Topic: Staying Safe on the Internet
AOB and Follow up

Current News, Issues and Questions

Anything to discuss?

Future Topics

Topic	Votes
Near field Communications (e.g. contactless payments)	5
Home Networks (smart homes)	4
Use of computing in Medicine	4
History of computer development	3
"Fix it" software for Windows	3
Key components of a modern computer & their interrelationships	3
Members' favourite magazines & websites	2
Quantum Computing	2
Future of Human Computer interface & cyborgs	2
PC boot sequence, BIOS, Disc structure	2
Use of computing in warfare	1

Presentation

Staying Safe on the Internet
(Including email)

Agenda

Safety on the Internet

- What is at risk
- Typical IT environment
- Virus types
- Risks & protection for situations:
  - At rest
  - Using Internet services
  - Email
  - Downloading files & applications
- Summarising

At Risk

Safety on the Internet

- Access to your bank account
- Bank transfers being made to the wrong account
- Bank card details being used
- Loss of data - ransom to recover
- Loss of other sensitive information - possibly leading to..
- Identity theft - debts being created in your name
- Unintended purchases
- Excessive Ads & promotions

Where is your sensitive Data?

Safety on the Internet

You may have sensitive data on:

- Personal Computer / tablet
- mobile phone
- (Home) Network Storage Device
- Online data stores (iCloud, Dropbox)
- Your Bank’s systems (bank, building society, investment platform)
- Pension systems
- HMRC online service
- GP practice / NHS
- Shopping systems (Amazon)
- Email host (gmail, BT)

- *Also in transit!*

Landscape to Consider

Safety on the Internet

Activities

- Systems at rest
- Access service using browser
- Access service using an app
- searching & “clicking around” the internet
- email
- using cloud storage
- Downloading files
- loading files from a USB stick

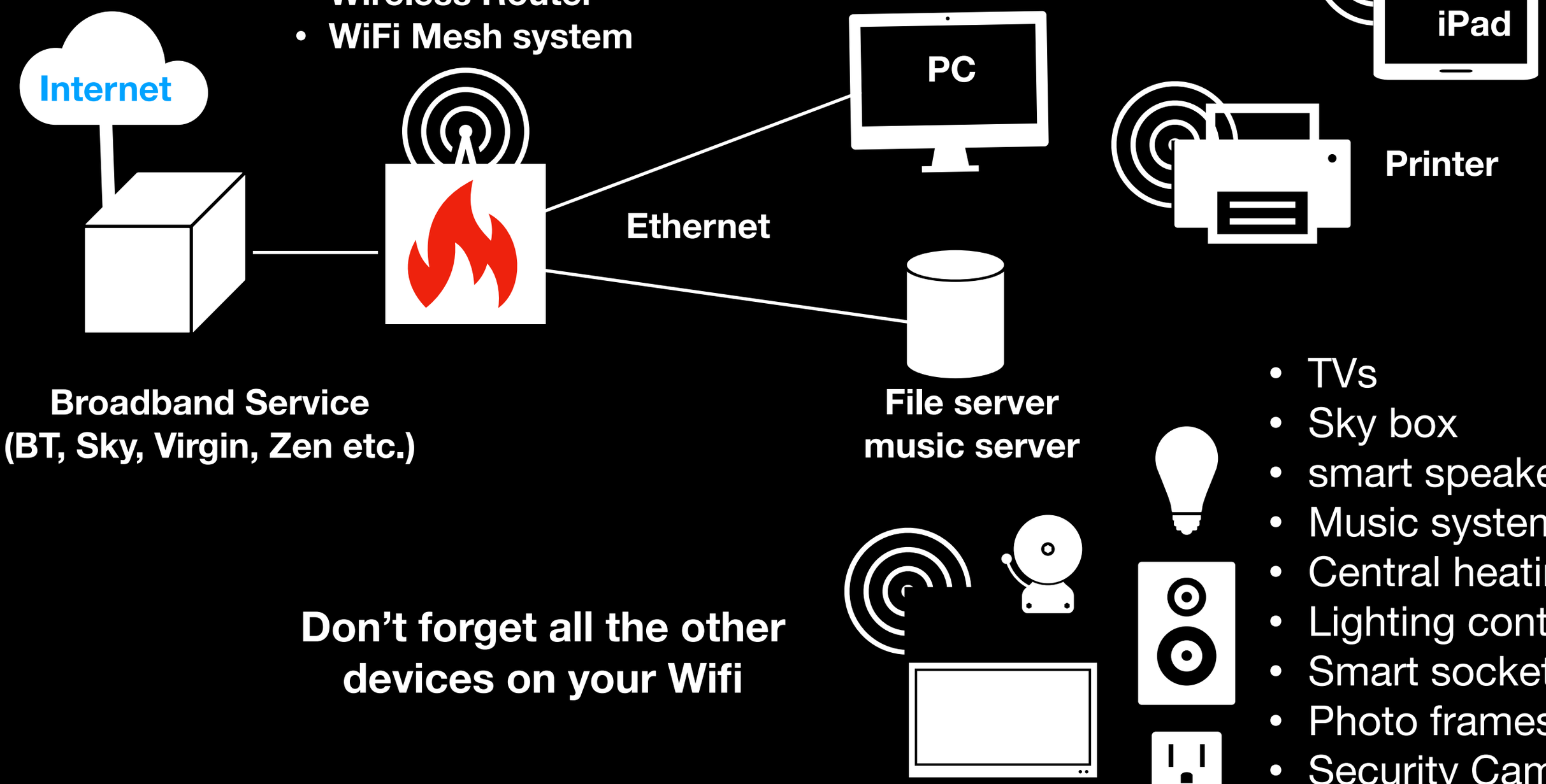
Environments

- At home
- Using mobile network
- Using public wifi

Home environment

Safety on the Internet

- Router with firewall
- Wireless Router
- WiFi Mesh system

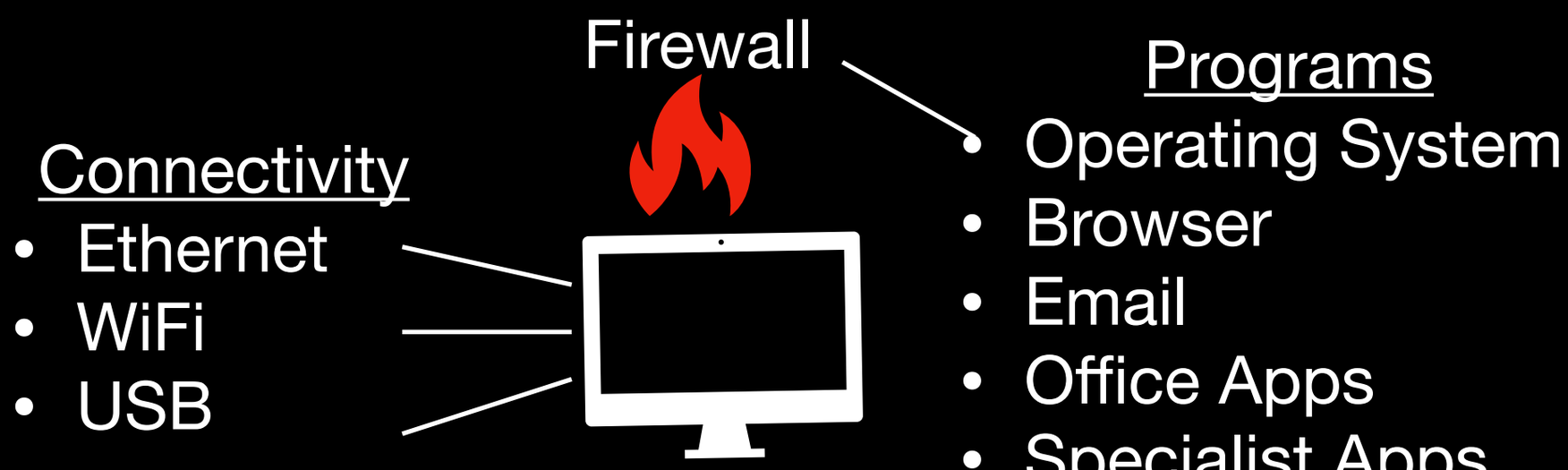


Don’t forget all the other devices on your Wifi

- TVs
- Sky box
- smart speakers
- Music system
- Central heating
- Lighting controls
- Smart sockets
- Photo frames
- Security Camera

Device Environment

Safety on the Internet



Virus Types

Safety on the Internet

- Macro Virus: Hide in MS Office.
- Trojan Horses: Disguised as normal program, tempting you to install.
- Browser Hijacker: Take over internet searches and direct you to pages you didn’t want.
- Web Scripting Virus: Blend into a popular website disguised as a normal link

Full explanation at:

https://www.buddycompany.com/post/types-of-computer-virus

Can “Your” Resting Systems be accessed?

Safety on the

- On the home network
  - PC
  - File server

Risks

- Connection request from “bad actor” on internet
- Virus on PC initiating a connection channel
- Device on home wifi hijacked
- File server is available to all devices on the home network

Protection

- Router Firewall: only allows connections originating from inside the wall
- WiFi: password protected
- PC Firewall: Only accepts connections to “enabled” applications

- Check router & WiFi set up for security
- Check File server security
- Keep PC software up to date
- Enable virus checking

Built in security is ample for normal use

Router Security Example

Security functions (firewall) of the FRITZ!Box

The FRITZ!Box offers you a completely closed firewall to protect against unwanted data from the internet. In the factory settings, all of the computers, smartphones, and other devices connected to the FRITZ!Box are already fully protected against attacks from the internet.

The FRITZ!Box's firewall provides the following security functions:

- The FRITZ!Box checks all incoming and outgoing data packets and automatically rejects unwanted data from the internet (Stateful Packet Inspection). This way **only data packets that are direct replies to previous requests reach the home network.**
- **None of the c** **rnet**, which means that it is not possible ed by IP Masquerading or Network Addres
- By default, all TC he internet to the home network. Therefc orts that could represent weak points for
- The FRITZ!Box u **ple NetBIOS) containing inf reaching the internet.**

Don’t Forget

- Check router admin password is strong
- Wifi Network name SSID should not be meaningful
- Make Wifi password strong

You can specifically set up port sharing for web servers or VPN servers, online games, and other applications that should be accessible from the internet.

If you want to make it more difficult to identify the FRITZ!Box with port scans, you can enable the option "Firewall in stealth mode" under "Internet > Filter > Lists > Global Filter Settings" in the FRITZ!Box user interface. Then the FRITZ!Box discards all queries from the internet to ports that have not been opened for sharing.

Can “Your” Resting Systems be accessed?

Safety on the

- Cloud Storage
  - Apple iCloud
  - Microsoft OneDrive
  - GoogleDrive
  - Dropbox….

Risks

- Data Centre being hacked
- Options available to allow file sharing
- Hacking a PC also gives access to cloud storage

Protection

- Data encrypted in transit and stored in encrypted format
- Encryption keys held securely

- check encryption is enabled
- Use very strong passwords
- Use 2 factor authentication where available.

Can “Your” Resting Systems be accessed?

Safety on

- Banking systems (bank, building society, investment platform)
- Pension systems
- HMRC online service
- GP practice / NHS

Risks

- Data Centre being hacked
- Your account being hacked using your id/password
- Bank System being spoofed to obtain your id/password etc (clicked link fro

Protection

- System should insist on strong passwords.
- Will always use encrypted link

- Use very strong passwords
- Use 2 factor authentication where available.
- Do not reuse passwords!

Using Secure Internet Services

From Home

- Banking systems (bank, building society, investment platform)
- Pension systems
- HMRC online service
- GP practice / NHS

Risks

- Domain spoofing
- PC virus leaking passwords etc
- insecure wifi network
- insecure router reconfigured

Protection

- encryption from PC device to Internet service
- password protection

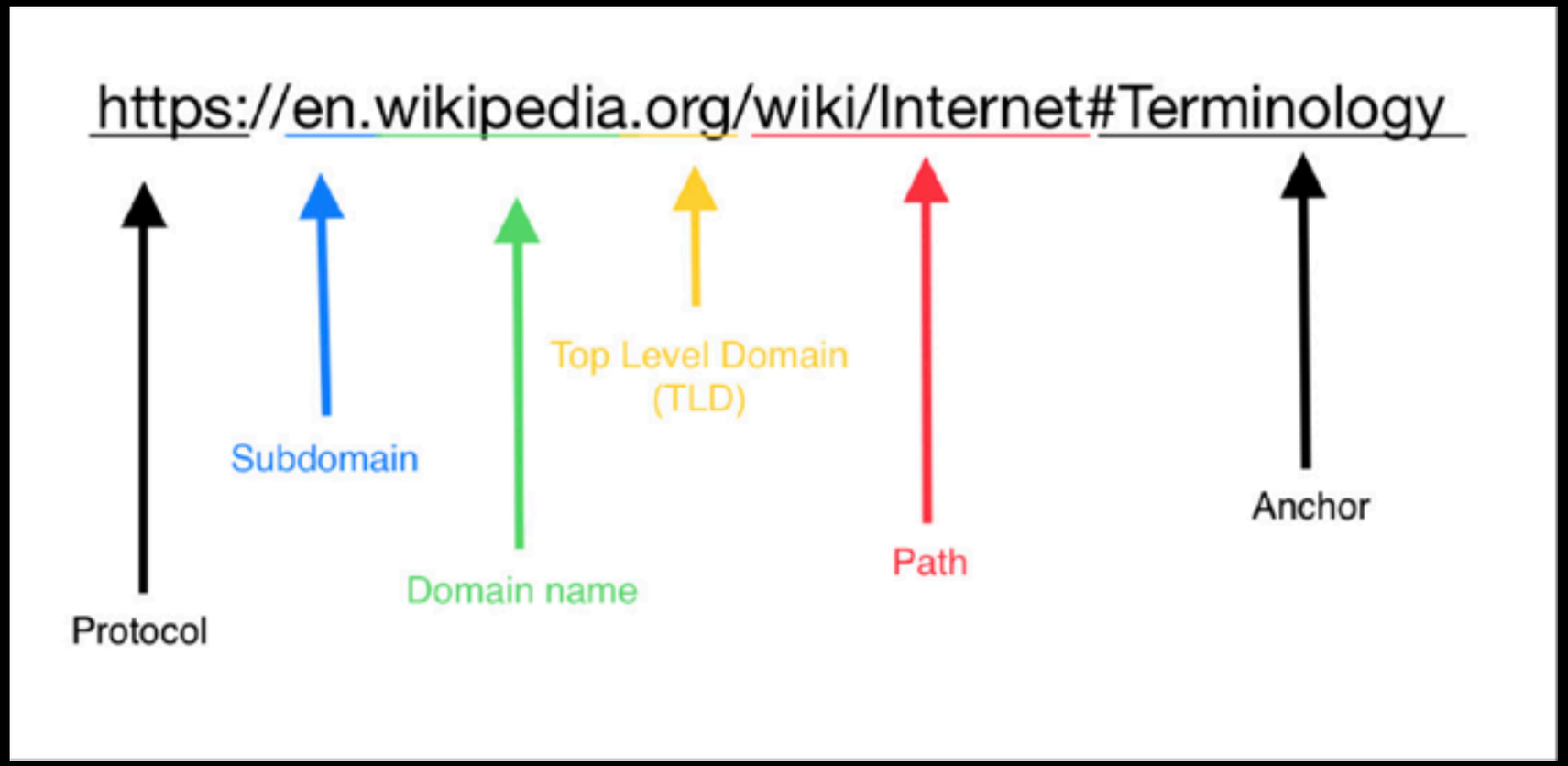
- Check browser padlock
- Check url
- Check router and wifi set up for security
- Don’t click on links to bank system

Domain Spoofing / URL Lookalike

Universal Resource Locator

URLs

- HTTP is the protocol used to transfer data
- HTTPS stipulates use of encryption
- Domain & top level domain define the website being connected
- Subdomain is a section of the website



- Check https is being used
- Check Domain and TLD are correct
- Watch for:
  - letter substitutes O-0, I-l, nn/m, 5/S
  - misspellings: insurrance,
- If in doubt, type the url yourself or Google the name of the company

Using Secure Internet Services

From Public hotspot

- Banking systems (bank, building society, investment platform)
- Pension systems
- HMRC online service
- GP practice / NHS

Risks

- Wifi hotspot may be malicious
- Can eavesdrop on all data.
- Can use “man-in-the-middle” to see passwords…

Protection

- Use mobile phone network instead
- Check validity of hotspot
- Use VPN to “tunnel” through

or

- Don’t do anything sensitive

Using Secure Internet Services

From Home or public hotspot

- Banking systems (bank, building society, investment platform)
- Pension systems
- HMRC online service
- GP practice / NHS

Using a banking app

- **Removes risk of url spoofing**
- **Ensures encryption always used**

n

- Wifi hotspo
- Can eavesc
- Can use “m
  to see pass

- Use mobile phone network instead
- Check validity of hotspot
- Use VPN to “tunnel” through

or

- Don’t do anything sensitive

Using email

From Home

- Email system
- Sending email
- Receiving email

Risks

- Email serve
allowing em
- Email addre
(if you click
- Incoming e
can be spo
- Incoming email can contain malware

- **Opening an email is safe - the email client limits actions to display**
- **Opening attachments is not safe**
- **Clicking a link is not safe**

(Email virus check should catch issues)

But…

Protection

email client to

admin

rs

king

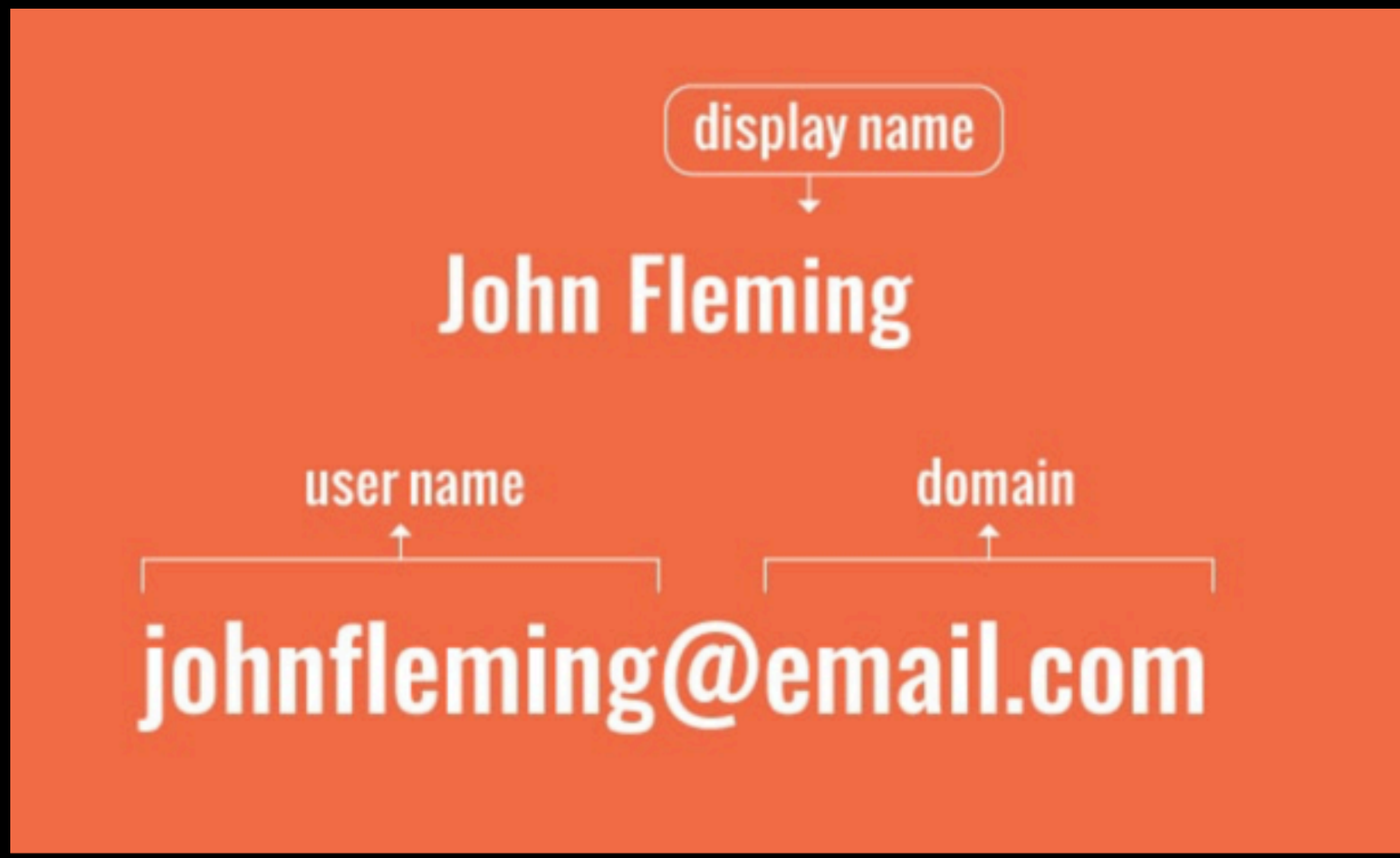
- Keep email client secure
- Avoid clicking “contact me” links
- Assume all incoming email is dubious
- Check incoming email addresses fully

Email spoofing

Safety on the Internet

Often SPAM emails have a display name that looks like a valid email address

- Every email client allows you to see the full email address - not just the display name.
- All your friends' addresses will have familiar domains
- All business will be business name .com or .co.uk or something mainstream
- If in doubt, google the email address



Email Risks - Phishing

Safety on the Internet

- Phishing emails can come from known contacts who have been compromised.
- To confirm if a sender's email is legitimate, verify with the sender directly using another form of communication.
- If the email claims to be from a company, go to the company's official website and call the number they have listed to confirm the email was actually from them.
- If the email claims to be from a friend, family member, coworker, contact them through text message or another messaging platform to check if they sent the email.
- If they claim that they did not send the email, they can take the necessary steps to warn other email contacts so they don't fall for the scam.

Email Scams

Safety on the Internet

Look for red flags:

An email from a scammer will often contain red flags that you can use to determine whether the email is legitimate:

- Urgent language, like “ACT NOW”
- Threats of dire consequences
- Misspellings and grammatical errors
- Offers that seem too good to be true
- Requests for personal information
- Links that don’t go to official websites

Loading Files Safely

Safety on the Internet

- Download from an internet source
  - Reputable source
  - Don’t ignore browser warnings
  - Use www.virustotal.com to check file BEFORE download
  - Run antivirus on pc
- From a USB
  - Reputable source? (your friend’s PC may be infected)
  - Run your virus check on the USB

Loading applications Safely

Safety on the Internet

Downloaded from an internet source

- Backup your PC
- Reputable source
- Run antivirus program

Risks by Device

Safety on the Internet

- iPhones do not need antivirus software unless tampered with
- Android phones have security but they are not as robust as Apple's (a recent report found that Android devices were responsible for 26% of all infected devices, including Windows PCs, IoT devices and iPhones.)
  - Security upgrades not as well managed
  - More freedom/flexible app sourcing
- Windows PCs remain the main target
- Apple Macs are also targets.

Advise Summary

https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online

Our top tips are:

1. Protect your email by using a strong and separate password
   Cyber criminals can use your email to access many of your personal accounts, leaving you vulnerable to identity theft.
2. Install the latest software and app updates
   Software and app updates contain vital security updates to help protect your devices from cyber criminals.
3. Turn on 2-step verification (2SV)
   2-step verification is recommended to help protect your online accounts.
4. Use a password manager
   Using a password manager can help you create and remember passwords.
5. Back up your data
   Safeguard your most important data, such as your photos and key documents, by backing them up to an external hard drive or a cloud-based storage system.
6. Three random words
   Use three random words to create a password that's difficult to crack.

Useful websites

Safety on the Internet

- National Cybersecurity Alliance: Stay Safe Online, a set of articles on internet safety https://staysafeonline.org/resources/
- Get Safe Online: UK's leading internet safety website. We provide unbiased, factual and easy-to-understand information on online safety. (includes check a website service) https://www.getsafeonline.org
- VirusTotal: Free virus check for files and urls - before you download or click. https://www.virustotal.com/gui/home/upload

Questions?