ICT Theory – Revision Presentation

Safety and Security

- 8.1 Physical Safety
- 8.2 e-Safety
- 8.3 Security of Data

Draw attention to:

- Book Chapter 8 Page 205 – Three subtopics
- Handout Questions – Three subtopics
- Class PowerPoint – Three subtopics
- Discussion
- Ppt
- To work on completing questions – you need your book and exercise copies

ICT Theory – Revision Presentation

Safety and Security

8.1 Physical Safety

1. Physical Safety - ICT?

2. The Computer Room

ICT Theory – Revision Presentation

Safety and Security

8.1 Physical Safety

Electrocution from spilling drinks

- Ensure all drinks are kept away from the computers, ICT labs or office desks.

Fire from sockets being overloaded

- Ensure plug sockets or extension cables are not overloaded.

Physical Safety Risks

Equipment overheating

- Ensure ventilation in the room is good and equipment is not covered whilst in use.

Tripping over trailing cables

- Ensure cable ducts are used to cover wires.
- Ensure cables are tucked away.

Strategies to minimise potential safety risks:

- **Regular maintenance of equipment to check if it is passing safety standards.**
- **Regular check of the state of cables/plugs to ensure there is nothing exposed.**
- **Use of wireless connections to eliminate the use of cables.**
- **Ensure potential trip hazards are under desks (bags, plug sockets).**

ICT Theory – Revision Presentation

Safety and Security

8.2 e-Safety

1. Why study e-Safety?
2. What is Personal Data?
3. Why bother protecting Personal Data?
4. How would you protect Personal Data?

ICT Theory – Revision Presentation

Safety and Security

8.2 e-Safety

Personal Data:

- Contact details (Phone number/email address)
- Address Details
- Personal Images
- Payment details including card and bank details
- Medical history
- Political views
- Family details
- Passwords

Why personal data should be confidential and protected:

- Users can be stalked or even kidnapped – status updates can alert people of your location at a particular time.
- Details can be stolen, copied or pass on.
- Users could be blackmailed/ threatened into doing inappropriate things.
- Customer details could be sold onto a third party.

How to avoid inappropriate disclosure of personal data:

- Ensure privacy setting in social media sites have been activated.
- Do not share data via social media or emails with strangers.
- Do not post inappropriate images or content.

Discuss why e-safety is needed:

These days youngsters are not fully aware of the **dangers the internet poses** and the **potential risks** they may put themselves under. For that reason eSafety lessons are taking place in schools to **educate young people about the potential risks of using the internet** appropriately so that they know how to **stay safe** whilst being online.

ICT Theory – Revision Presentation

Safety and Security

8.2 e-Safety

1. How do we use the internet?
2. How should you keep yourself safe on the internet?

3. What do we use email for?
4. How should you protect yourself when using email?

ICT Theory – Revision Presentation

Safety and Security

8.2 e-Safety

Minimise the Potential Dangers

Personal Use of Internet

- **General browsing – keeping up to date with current affairs.**
- **Researching for school projects.**
- **Online shopping/banking**

- Only use **trusted websites** or those recommended by teachers.
- Only use a **student friendly search engine** with **safety filters**.
- **Restrict access** to certain content via ISP or filtering software.

Use of Email

- **To keep in touch with friends, family and co workers.**
- **To share information including attachments - Images, Presentations etc.**
- **To get in touch with organisations.**

- Only email people already known to you or from your **contacts list**.
- Think before opening an email from an **unknown person**.
- Be careful about emailing your **school's name or a picture of yourself in school uniform**.

ICT Theory – Revision Presentation

Safety and Security

8.2 e-Safety

1. What is meant by social media? Who uses it?

2. How can you protect yourself on Social Media?

3. Online Gaming – what is it?

4. What advice would you give to a primary school student who is starting out with online games?

ICT Theory – Revision Presentation

Safety and Security

8.2 e-Safety

Minimise the Potential Dangers

Use of Social Media

- **Personal Use:**
  - **Share information about yourself to your friends and followers.**
- **Business Use:**
  - **Promotion/Awareness**

- Know how to **block and report** unwanted users in chat rooms.
- Never give out any **personal information** online.
- **Never arrange to meet strangers** especially in a secluded place.
- Keep **adults informed** about your use of social media.

Online Gaming

- **Online gaming is now very popular over many platforms. More games are now providing multiplayer options with some games.**
- **Maps especially created for online gamers.**

- Never use **real name** when playing games online.
- Use **appropriate language** when using headsets and communicating with other gamers.
- Only **play online with trusted friends**.

8.3 Security of Data

1. What is a Hacker?

Hacking

2. Why do some people hack?

3. How do you protect yourself from hackers?

ICT Theory – Revision Presentation

Safety and Security

8.3 Security of Data

What is Hacking?

- To gain unauthorised access to a computer system without the user knowledge or permission.

Effects of Hacking?

- To delete, corrupt, copy and edit files. Sensitive Data could be sold to competitors.
- Identity theft – to steal users identity.
- To expose a company (for example wiki leaks).
- To cause disruption and stop production.

Hacking

Strategies to prevent hacking to protect data

- Use of firewalls – sometimes part of the operating system.
- Use of strong passwords which are frequently changed.
- Use of protection software to detect and block possible hacking attempts.
- Hire a professional hacker to test the weaknesses of your system.

Safety and Security

8.3 Security of Data

1. What is a computer virus?
2. Why should viruses worry us?
3. How do we prevent them?

Computer Virus

ICT Theory – Revision Presentation

Safety and Security

8.3 Security of Data

What is a computer virus ?

A computer virus is a piece of programming code/software which can install and replicate it self on to a computer system without the user's permission.

Effects of a computer virus ?

- **Causes the computer to crash – become slower**
- **Sometimes files can be deleted – leads to computer malfunction.**
- **Data files can be copied by the hacker or the files could be corrupted.**
- **Could stop production until the virus has been quarantined.**

Strategies to prevent computer virus

- **Install <u>antivirus software</u> and <u>regularly update it</u>.**
- **Do not <u>use software</u> or <u>USB</u> from <u>unknown sources</u>.**
- **Be careful about <u>clicking on links</u> from <u>untrusted websites</u>.**
- **Be careful about <u>downloading attachments</u> from <u>unknown email addresses</u>.**

Computer Virus

Downloaded exe (executable) files could also be a virus when they are installed by double clicking on them.

ICT Theory – Revision Presentation

Safety and Security

8.3 Security of Data

1. What is Spyware?
2. Why should they worry us?
3. How do we prevent them?

Spyware

ICT Theory – Revision Presentation

Safety and Security

8.3 Security of Data

What is Spyware?

Is a software which can monitor your use of the computer (internet browsing) and monitor and log key pressed.

Effects of Spyware?

Spyware software will send the data back to person who planted the spyware software on your computer. This could include personal details like passwords and banking account information.

Spyware software could also install additional software to read cookie data and change web browsing preferences.

Strategies to prevent Spyware

- **The use of anti spyware software which is regularly updated.**
- **The use of a pointing device to select characters when entering sensitive data.**

Spyware

ICT Theory – Revision Presentation

Safety and Security

8.3 Security of Data

1. What is Phishing?
2. Why does it affect us?
3. How do we prevent Phishing?

Phishing

ICT Theory – Revision Presentation

Safety and Security

8.3 Security of Data

What is Phishing?

The recipient will receive an email which looks legitimate. The email will normally request the user to update their details which could be their password or payment details. To update the users details they will have to click on a link which will take them to a fake website.

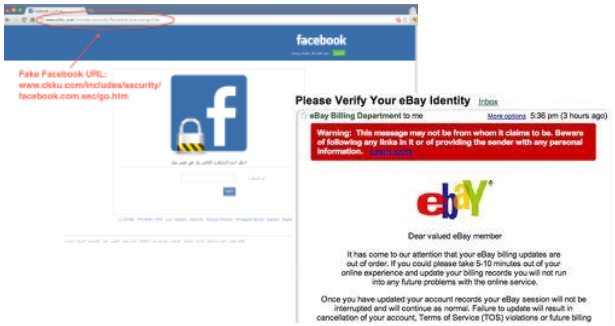
Effects of Phishing?

The user will be tricked into entering their details into a fake website. The sender of the initial email will have gained personal details from the user. These details can be used fraudulently or for identity theft.

Strategies to prevent Phishing

- Use a filter on your email account so that only emails from an allowed users appear in your inbox.
- Always double check the URL and email address.

Phishing

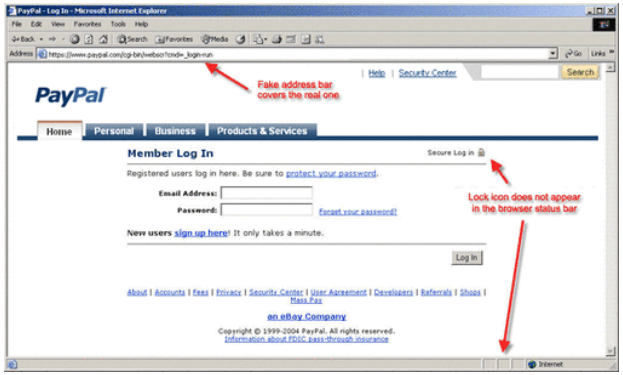


Safety and Security

8.3 Security of Data

Pharming

1. What is Pharming?
2. Why does it affect us?
3. How do we prevent Pharming?



ICT Theory – Revision Presentation

Safety and Security

8.3 Security of Data

What is Pharming?

A malicious code installed onto a web server or computer will redirect users to a fake website even though they have typed in a legitimate URL address.

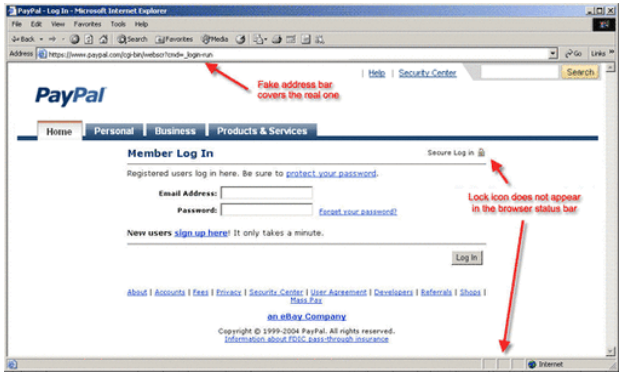
Effects of Pharming?

The fake website will look like the real website (websites tend to look like a trusted websites to deceive the user). Users will be tricked into entering their personal details. Like Phishing this can lead to fraud or identity theft.

Strategies to prevent Pharming

- **Anti spyware software could eliminate pharming code from a computer.**
- **Always double check the URL to see if is the same one you typed in.**

Pharming



8.3 Security of Data

Smishing

1. What is Smishing?
2. Why does it affect us?
3. How do we prevent Smishing?

ICT Theory – Revision Presentation

Safety and Security

8.3 Security of Data

What is Smishing (SMS Phishing)?

Users will receive fake SMS (text) messages claiming they have won some sort of prize. Text message will appear to come from a legitimate company. To claim the price users will have to call a premium phone number or go to a website and give personal details.

Effects of Smishing?

The effects are very similar to Phishing and Pharming where personal details will be obtained from users. However users could incur additional costs when they ring the premium number to claim a prize.

Strategies to prevent Smishing

- **<u>Double check</u> the SMS message – check for spelling mistakes.**
- **Check the <u>link of the website</u> to see if it is <u>legitimate</u>?**
- **Contact your <u>bank directly</u> If you are requested to change some details.**

Smishing

Vishing: Uses a voice messages which tricks users into calling a premium rate telephone. Voice mail may sound legitimate and may request for user to update their details.

ICT Theory – Revision Presentation

Safety and Security

8.3 Security of Data

Spam Email

1. What is Spam Email?
2. Why does it affect us?
3. How do we prevent Spam?

ICT Theory – Revision Presentation

Safety and Security

8.3 Security of Data

What is Spam Email?

Spam (junk) email is sent out to recipients from a mailing list. The email could be part of a phishing scam or could be to promote certain products. They are basically unwanted emails.

Spam Email

Effects of Spam Email?

If a spam email is part of a phishing scam then there is a chance your details could be obtained. The network could also become slower or unresponsive if there is a lot of unnecessary traffic flooding the network.

Strategies to prevent Spam Email

- **Use a <u>junk email filter</u> to stop spam email coming into the inbox.**
- **Do not <u>sign up for any commercial mailing lists</u>.**
- **Do not <u>reply to spam email</u>.**
- **<u>Untick the check box</u> if you are asked to give your email to a <u>third party</u>.**

8.3 Security of Data

1. What is Credit Card Fraud?
2. Why does it affect us?
3. How do we prevent it?

Credit Card Fraud

ICT Theory – Revision Presentation

Safety and Security

8.3 Security of Data

What is credit card fraud?

Online credit card fraud is when a user is tricked into giving their personal and financial information. This could be via phishing, pharming or the use of spyware software.

Effects of credit card fraud?

When a users account has been breached (credit/debit card details have been obtained)then unauthorised purchases can be made. Also money can be transferred out of the account.

Strategies to prevent credit card fraud.

- Have a strong password on your account.
- Ensure website has a secure connection.
- Install and update spyware software.
- Regularly check bank statement for any suspicious activity.

Credit Card Fraud

8.3 Security of Data

1. What is Biometrics?

2. Name different types of biometrics!

3. What are their advantages & disadvantages?

ICT Theory – Revision Presentation

Safety and Security

Biometrics is a method of authentication. It relies on unique characteristics of human beings. Biometrics data is difficult to copy and requires the user to be present so that this method of authentication can be used.

		Advantage	Disadvantage
	**Fingerprint Scans:** **Users will have press their finger against the scanner. Finger prints are compared against those stored in the database.**	• Very easy to use. • Very high accuracy. • Small storage requirements for biometric data.	• If the skin is damaged then it may be difficult for the reader to read and recognise the fingerprint.
	**Retina/Iris Recognition:** **Scans use infrared light to scan unique patterns of blood vessels in the retina.**	• Very high accuracy. • No way to replicate a users retina.	• Very intrusive • Expensive to setup • Takes a while to scan.
	**Face Recognition:** **Physical facial features are scanned and compared to the information held in the database.**	• Non-intrusive method • Cheap technology	• Physical features can change over time with age.
	**Voice Recognition:** **User will use speak which will compare the voice to one held on the database.**	• Non-intrusive method • Cheap technology • Verification is very quick.	• Very low accuracy. • Users voice could be affected by an illness.

Protection - Summary

ICT Theory – Revision Presentation

Safety and Security

8.3 Security of Data

To protect your **personal data from being obtained** you need to be **fully aware of phishing, pharming and vishing scams**. There are always **signs** which should cast doubt to whether you should **disclose your personal information**. Also the use of **an updated spyware software** would help improve security on your computer.

Any attempt to obtain illegal information should be reported to the authorities.

Why is it Used

Firewall

- **Firewall provides security to a computer or network**.
- Is **located between the computer and internet connection**.
- Firewalls will **examine network traffic** and **block and alert users to potential risks**.

Passwords and User Name

Passwords are a method of authentication. They are used frequently online when logging onto user accounts. If passwords are breached then your account may be hacked. Details could be shared with other users of the internet.

ICT Theory – Revision Presentation

Safety and Security

8.3 Security of Data

Encryption is the process of converting information into a form that is meaningless to anyone except holders of a **'key'**.

Encryption Key

1	2	3	4	5	6	7	8	9	10	11	12	13
A	B	C	D	E	F	G	H	I	J	K	L	M
14	15	16	17	18	19	20	21	22	23	24	25	26
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Hello → Data is Encrypted → 85121215 → Data is Decrypted → Hello

Data in scrambled into a meaningless format. Even if it is intercepted it would mean nothing to hackers.

Data is now in a format which can be understood.

ICT Theory – Revision Presentation

Safety and Security

8.3 Security of Data

Cloud: **Online storage medium used to backup files. Files can be accessed from any device with an internet connection.**

Moderated Forums: **Online discussion forum where all posts are moderated by an administrator.**

Un-Moderated Forums: **No measures are place to moderate posts by users.**

Issues Related to Security of Data

- Data has been lost in the past during a routine backup.
- Celebrity data has been hacked and shared including images.
- The security of the building where the servers are held and access rights to employees could effect the security of the data.

Security of Forums:

Moderated forums are more secure than un-moderated forums as posts are regularly checked by the admin. Inappropriate posts which could be offensive can be deleted.

Digital Certificates

They are used to **verify the identity of the sender** in an online business transaction. It also provides the opportunity for the **receiver to give an encrypted response**.

ICT Theory – Revision Presentation

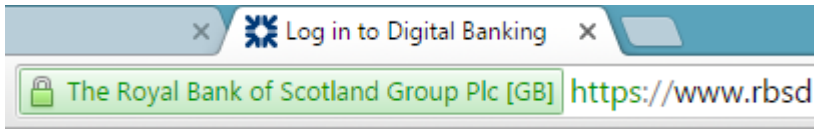
Safety and Security

8.3 Security of Data

Secure Socket Layer (SSL)

- **Using a secure connection ensures data is kept safe when sending sensitive information.**
- **Secure websites encrypt information before sending it to others.**
- **Only the computer on the other end can read and understand the data.**
- **Websites which depend on security can have their websites reviewed and validated by companies called certificate authorities. These reviews will ensure the website is secure.**

Features of a web page that identify it as using a secure server



S will show after **http** in the URL address – for example **https://www.ebay.co.uk**

Padlock will be shown on browser to show users the webpage is secure.

Colour and **company name** will be shown in the address bar in the **colour green** once it has been validated by the certificate authorities as being secure.

Give your neighbour advice about:

- Usernames and Passwords
- Online Safety
- Cyberbullying
- Meeting online friends
- Photographs and Webcams
- Emails, USB sticks, Viruses, Downloads, etc