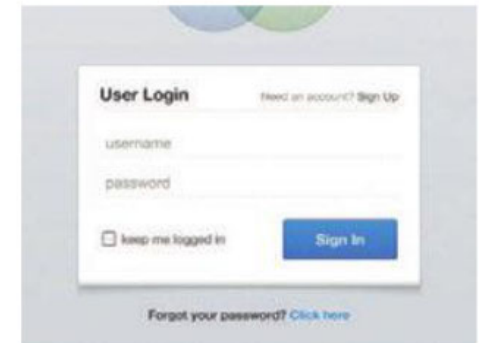


KEEPING DATA SAFE FROM SECURITY THREATS




- Access level
 - different levels of access in a computer system allowing a hierarchy of access levels depending on user's level of security
 - E.g. read/write/execute
- Anti-malware
 - Antivirus (Already in chapter 4)
 - Anti-spyware
 - It scans, detects and removes spyware



▲ Figure 5.13 Access level log in screen

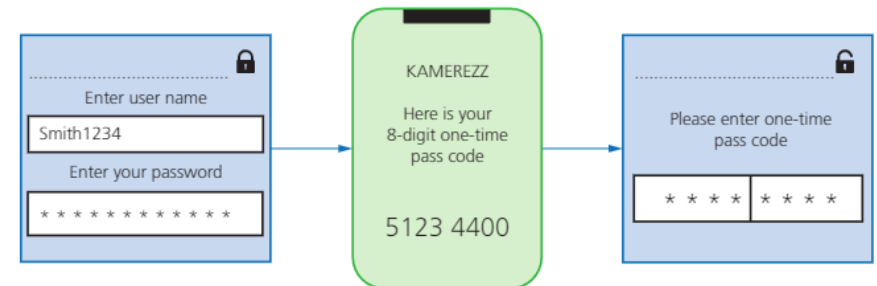
All recent items

Filters ▼

	Threat removed or restored 23/12/2021 23:49	Severe
	Threat removed or restored 23/12/2021 17:06	Severe
	This app has been blocked 9/9/2021 22:48	Low

KEEPING DATA SAFE FROM SECURITY THREATS

- Authentication : the ability of a user to prove who they are by using
 - Something you know : password
 - Something you have : mobile phone
 - Something which unique to you : biometric
- Two-step verification
 - requires two methods of authentication to verify who a user is
 - E.g. OTP (One Time Password)
 - Users have to has password and mobile phone(something you have to verify)



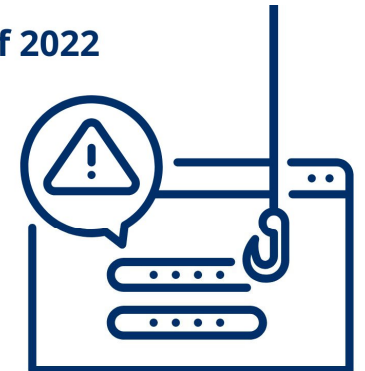
KEEPING DATA SAFE FROM SECURITY THREATS

• Usernames and passwords

- It requires both username and password to input correctly to access the data
- strong passwords should contain:
 - at least one capital letter
 - at least one numerical value
 - at least one other keyboard character (such as @, *, &, etc.)
 - an example of a strong password would be:
Sy12@#TT90kj=0
 - an example of a weak password would be: GREEN

The Top 20 WORST Passwords Of 2022

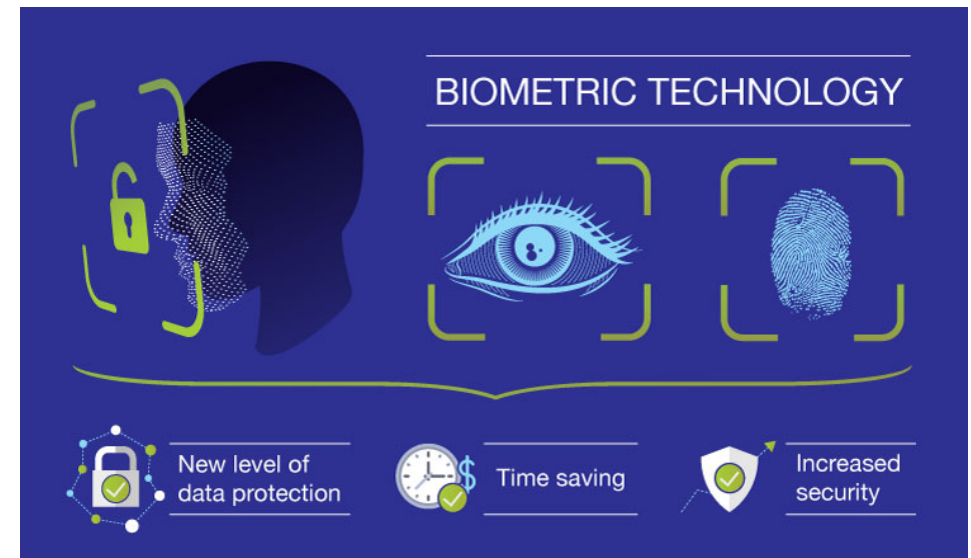
- 123456
- 123456789
- qwerty
- password
- 12345
- 12345678
- 111111
- 1234567
- 123123
- qwerty123
- 1q2w3e
- 1234567890
- DEFAULT
- 000000
- abc123
- 654321
- 123321
- qwertyuiop
- Iloveyou
- 666666



KEEPING DATA SAFE FROM SECURITY THREATS

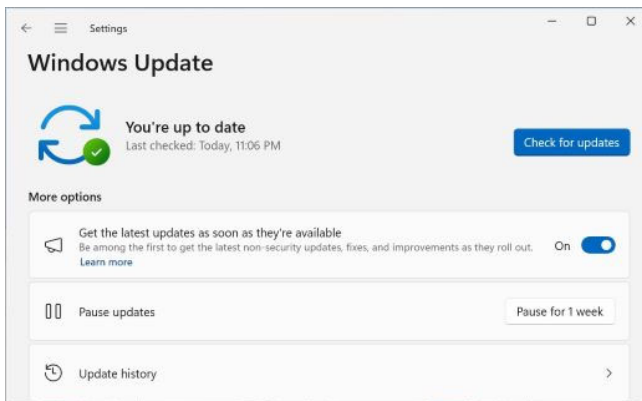
- **Biometrics**

- It relies on certain unique characteristics of human beings e.g. fingerprint, retina, face and voice
- Biometrics are difficult to be duplicated
- Users cannot forget to bring their biometric
- Problems
 - Sickness : wound on finger, have a cold
 - Wearing contact lens, glasses, mask
 - Privacy issue



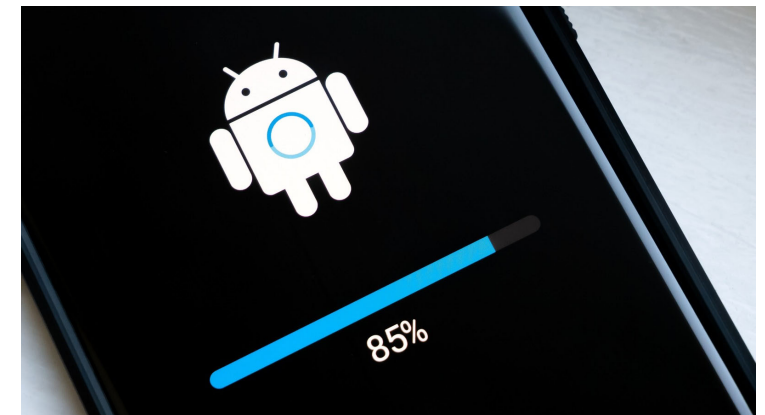
KEEPING DATA SAFE FROM SECURITY THREATS

- Automatic software updates
 - Since software might have errors weaken the security, programmers need to release patch to fix the problems
 - computers and mobile phones/ tablets is kept up-to-date. Sometimes this is done overnight or when you log off the device



This update provides important bug fixes and security updates and is recommended for all users.

For information on the security content of Apple software updates, please visit this website: <https://support.apple.com/kb/HT201222>



KEEPING DATA SAFE FROM SECURITY THREATS

- Checking the spelling and tone of communication and URL links
 - When emails are sent to you, there are actions you always need to take before opening them or activating any links in them
 - Check out the spellings in the email and in the links; professional, genuine organisations will not send out emails which contain spelling or major grammatical errors (for example, Amazzon.com)
 - Carefully check the tone used in the email message; if it is rushing you into doing something or if the language used seems inappropriate or incorrect, then it could be a phishing email or worse.
 - The email address itself; no legitimate company will use an email address such as: @gmail.com
 - The tone of the email and bad spelling of words is a clear indication of a potential scam
 - Misspelling of domain names in a link are very common errors found in emails sent by scammers and fraudsters www.google.com
 - Suspicious links

From: PayPal <paypal@customer-notice55.com>
To: PayPal user 551-121-998
Sent: Feb 1st 2021 @ 10:55
Subject: Compromised Account [CaseID Nr: KX-003-551-121-998]

Dear Customer

We need you help to resolve issue with account. We have temporarily stop account due to problem's. Unusual account activity on PayPal account means action need be taken immediately. If your not sure this was you, an unauthorized user might be trying to access your accounts. Please to log in here to change your password:

[LOG IN HERE](#)

NETFLIX

Failed subscription renewal notice.

Your bank has rejected our last attempt to collect your monthly subscription. Please click on the link below to review your billing details.Thank you.

[CONTINUE>>](#)

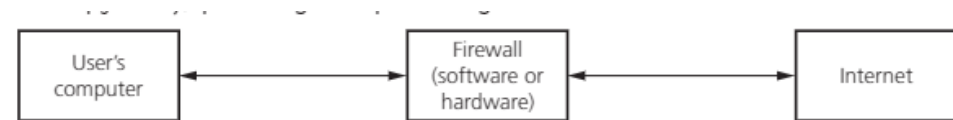
When you hover over this link you can see that the destination is a website with the address: <http://billing.com/id1234121XA3>

there is no mention anywhere of the company in this URL– very high chance it is a scam to try and collect your personal details

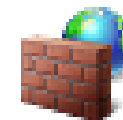
KEEPING DATA SAFE FROM SECURITY THREATS

•Firewall

- Software or hardware sits between the user's computer and an external network. It monitors in/out traffic and check against criteria. If it fails, blocks that traffic
- How does it work
 - Examine the traffic
 - Block unauthorised traffic from the user's computer
 - Allow traffic to access if they pass criteria
 - Give warning to the user if an intruder is found



▲ Figure 5.21 Typical firewall set up



Windows Firewall
[Check firewall status](#) |

KEEPING DATA SAFE FROM SECURITY THREATS

- Proxy server

- It acts as an intermediate between the user and a web server

- Features

- allows internet traffic to be filtered; it is possible to block access to a website if necessary

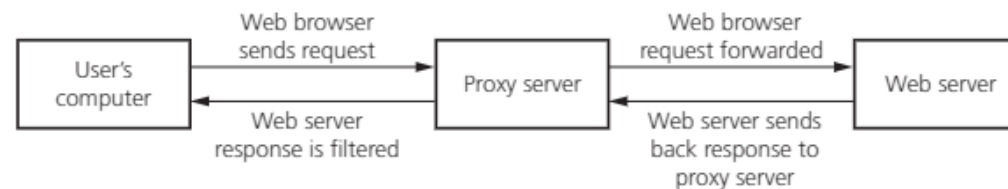
- keeps users' IP addresses secret which improves security

- if the internet traffic is valid, access to the web server is allowed

- if the internet traffic is invalid, access to the web server is denied

- prevents direct access to a web server by sitting between the user and the web server. if an attack is launched, it hits the proxy server instead – this helps to prevent hacking, DoS, and so on

- by using the feature known as a cache, it is possible to speed up access to information/data from a website; when the website is first visited, the home page is stored on the proxy server; when the user next visits the website, it now comes from the proxy server cache instead, giving much faster access



KEEPING DATA SAFE FROM SECURITY THREATS

- Privacy settings

- the controls available on web browsers, social networks and other websites that are designed to limit who can access and see a user's personal profile
- a 'do not track' setting; the intention here is to stop websites collecting and using browsing data which leads to improved security
- safer browsing; an alert is given when the browser encounters a potentially dangerous website (the undesirable website will be in a 'blacklist' stored on the user's computer)
- web browser privacy options (e.g. storing browsing history, storing cookies)
- website advertising opt-outs; a website may be tracked by any number of third parties who gather information about your browsing behaviour for advertising purposes apps; for instance, the sharing of location data in map apps can be switched off

KEEPING DATA SAFE FROM SECURITY THREATS

- Secure Sockets Layer (SSL)
 - It is a type of protocol that allows data to be sent and received securely over the internet by using encryption
 - It uses https
 - Uses of SSL
 - Online banking
 - Online shopping
 - Email
 - Cloud storage
 - Social network

QUESTION

- Describe what is meant by a DDoS attack and suggest one security device that can be used to help prevent a DDoS attack

QUESTION

Identify a security solution that could be used to protect the computer from a computer virus, hacking and spyware.

Each security solution must be different.

Threat	Security solution
Computer virus	
Hacking	
Spyware	

QUESTION

- Describe what is meant by phishing and pharming. 6 marks