Stretch Project Research

Passwords

History

Passwords have been around for centuries. One of the earliest uses was with Romans, to distinguish between their friends and their enemies. These were called watchwords. They would split the whole army into different sections and pass around the watchword between these soldiers. All watchwords would have to be returned and this was a good way for them to keep track if there had been a leak. The tribune would be able to identify which section had not returned their watchword and track down the soldier that was to blame and punish them.

The first use of a computer password was created by Fernando Corbató, at MIT in 1961. The university had a huge Compatible Time-Sharing System (CTSS), but this system only had one mainframe and one single disk. So, Corbató created a password system so that the scholars could keep their files private on the CTSS.

Protection

Password protection begins with creating your password. A strong password means that your accounts can be much more secure and you are much less likely to be hacked.

Tips for what not to do for your password:

Don’t use a dictionary word, too simple and is easily cracked

Examples: ‘password’, ‘computer’, ‘remember’

Don’t use personal information, can be research to guess, usually reasonably simple, and if the password does get cracked that personal information can be used in other places like security questions or other passwords

Examples: ‘Julie0602’, ‘Scruffy’, ‘bday0912’

Don’t use a series of symbols, letters or numbers, these are too simple and can easily be cracked as it’s easy to guess

Examples: ‘abc123’, ‘qwerty’, ‘!”£$1234’

Don’t switch numbers, symbols or capitals for letters in a dictionary word, easy to guess as it’s such a common way to make a simple password look more complex

Examples: ‘pa$$w0rd’, ‘r3mEmbeRm3’, ‘l0G1n’

Tips for what to do with your password:

Do use a passphrase, this can be a string of random words in plain text that is longer so that it’s harder to crack

Examples: ‘jugglernumberpasstruth’, ‘afraidcreaturecorrectraccoon’, ‘loveablespiderchillytable’

Do use a sentence that is easy to remember and only use the first letters of each word, this will look like a jumble of characters and will be harder to crack as it doesn’t follow a pattern

Examples: ‘iLecaG2tS’ – I like eating chocolate and going to the shops, ‘mGltWw1’ – My grandmother lived through WWI, ‘Ih3daIw5C’ – I have three dogs and I want three cats

Do use longer passwords, the longer a password the more characters there are to crack which will take longer for someone trying to discover your password

Tips for keeping your passwords safe:

Do use different passwords for different websites, if one of the websites you use does get hacked or one of your passwords does get cracked, it will only affect one account rather than multiple, it keeps the problem isolated and means that you only have to change the password and information on that account

Don’t write your passwords in an easy to find place, this could be physically or virtually, like writing them on a sticky note that you keep at your desk or on your laptop and this can also mean not on a regular note on your phone or in a word document on your computer. Anyone can find these easily and they aren’t protected in the same way as they could be if you use a password manager or just remember them

Don’t use your passwords for your any of your accounts while on a public network, like Wi-Fi in a coffee shop. These connections can be watched by hackers as they are normally open to anyone, hackers can also pretend to be these connections and you could be connecting to a hacker without realising, so using any account passwords while on these networks could compromise them

Don’t use your passwords for any of your accounts on a public computer or a computer that you don’t trust, public computers can be used by anyone, which means that a hacker could have compromised the computer and could be recording your key presses and get your passwords from your accounts that way

Don’t change your password too often, normally people are told to change their passwords often, but a research study found that people tend to make their passwords easier as they have to change it so frequently and will end up only changing a little bit of this simpler password. The only reason that you should have to change your password is if there has been a data breach

Do keep up to date with data breaches, this can inform you of when certain accounts have been compromised and you should change your password immediately. You do have to be careful with these, because hackers will try and trick you with data breaches by sending you an email saying there has been a data breach when none has occurred, and make you go through the link to change your password, and they can record what you put in and have your password. Make sure to research any apparent data breaches to ensure that they are real and you are not being scammed

Don’t save your passwords on your browser, although convenient and in some browsers quite secure, it can cause a lot of problems if your laptop or phone is stolen. This means that whoever the thief is can use your passwords to get into all of your accounts if you save them all. Depending on your browser, your passwords may be available to be viewed in plain text which makes their job even easier, there are also different tools that can compile passwords that aren’t viewable on browsers and they can get your passwords this way. It’s safer to keep your passwords in a different place and not save them to your browser

Applications

Password Strength Analyser

Password Manager

Other Examples

Advanced

Personal Data

History

Problems with data privacy can be traced back to WWII. The Nazis abused data privacy when they wanted to identify minority groups and Jews. This misuse of data privacy continued when Germany was split in two after WWII, into East and West. In East Germany, the Stasi, their secret police, put the citizens of East Germany under heavy surveillance. This included checking their mail and also bugging their houses.

Around this time, the first data protection law in Germany came about. West Germany introduced a law in 1970 for data privacy, as a reaction to the events happening in East Germany. This was then followed by the 1977 Federal Data Protection Act, which sought to protect the Germans’ data against abuse in storage, distribution, modification, or deletion. This law was not able to be enforced in East Germany until the wall was taken down in 1989.

Meanwhile, in France, government was ploughing ahead with privacy laws for their country. In 1978, they decreed their own law for data protection, the Data Processing, Data Files, and Individual Liberties Law, which made it illegal to process private information, automatically or non-automatically, with a few exceptions.

This law paved the way for a law for the European Union to be introduced, and be more of a catch-all instead of each country having an individual law. This law was the European Data Protection Directive in 1995, and was the predecessor for the General Data Protection Regulation (GDPR).

The GDPR was introduced in 2018, and has been very influential in the change of data protection in the European Union. It increases potential fines for companies that breach it, makes the data that companies have on individuals more transparent, and helps these people prevent the collection of unnecessary data.

Protection

A big part of your personal data now exists online, in the form of social media. Which means you should keep a close eye on all of your social media presence because that information can be abused by others.

Tips for social media presence:

Don’t share too much of your personal information, people can use this for security questions that you use for your accounts, so not posting all of your personal data online can help

Do customise your privacy settings, make sure to try and keep your settings as private as possible so that people can’t find out information about you without knowing you. Meaning strangers can’t view your profiles without you allowing them to

Do check these privacy settings, social media sites tend to change their privacy settings frequently and can change your settings without you realising, so checking that your privacy settings are staying the same is a good practice

Encrypt your data, this makes your data unreadable unless you have the key to decrypt it

Applications

Encryption Program

Other Examples

Advanced

Hacker Attacks

Phishing

Definition

A phishing attack uses email, message or a pop-up to lure users into revealing sensitive and personal information like their passwords for certain accounts or credit card details. These attacks will have a message that will tempt the user to click on a link, these links will have been set up by the hacker to steal the information that they have gotten the user to input into the sight.

This could be creating a fake PayPal form to make it look like your credit card needs changed, but what really happens is that they’ll watch what you type and can steal your login credentials for PayPal as well as your credit card details.

In these instances, hackers can do more than just steal your information. They can also send out phishing emails from the compromised email account to the contacts in the address book and creating a chain to continue their attack. Malicious code, executed due to the phishing email and clicking on the link, can also take control of the user’s computer, being able to do whatever the user was able to do, this is known as pharming.

History

The concept and term of phishing was first introduced in the 90s, with America Online (AOL). People consider this the first phishing attack to happen. A group of hackers and pirates decided to create a group called the warez community, and executed this attack.

To execute this attack, they used a random number generator to create fake credit card numbers to create a phony AOL account. They would run these fake credit card numbers through the AOL system to create an account and what for a hit on one of the fake numbers.

Once the account was created, they would then spam other AOL users with emails from these phony accounts to try and get sensitive information from them.

Protection

Applications?

Other Examples

Advanced

Trojan

Definition

Trojan viruses, also known as Trojan horse viruses, are innocent looking programs that once they have been downloaded and installed, run malware on the user’s computer and infects it. Named after the Trojan horse trick that was used by the Ancient Greeks, in the 12th Century, to capture Troy.

Typically, these viruses are spread via messaging apps, email, or web downloads. Once the virus has been installed, it creates a backdoor for the hacker and they can now do whatever the user could do on the user’s computer.

A backdoor is a way to access a computer system without having to go through any of the security measurements put in place like login and passwords. So, this is how the hacker would be able to get in to control a user’s computer.

History

The first appearance of a Trojan virus was back in 1986, named the PC-Writer Trojan. Spread through a download, this virus pretended to be the newest version of the word processor PC-Write to get people to download and install the Trojan virus.

After launching the Trojan application, the virus would format the disk and delete all the data off the user’s disk, leaving them with nothing.

Protection

Applications?

Other Examples

Advanced

Keylogging

Definition

A keylogger, also known as a keystroke logger or a system monitor, is used to record every keystroke and mouse click made by the user at all times. This is commonly known as a spyware tool, as it’s used to spy on the user’s computer. Using this tool, hackers are able to record everything the user types, meaning they can collect personal data, credentials, and sensitive data. This can include credit cards and login details.

History

The first keylogger was in fact a piece of hardware, used for keylogging. In the 1970s, Soviet spies implanted a bug in the IBM Selectric typewriters of US diplomats, to track what they were typing. Using this piece of hardware, they were able to monitor classified documents.

Consisting of miniaturised circuits, placed in a metal bar, this implant was not able to be detected by the naked eye and could only be seen with an X-ray. Once the implant was placed in the typewriter, it was able to record the position of the little ball that would print the characters onto the typewriter paper.

These results could then be sent to Russia in real time.

Protection

Applications?

Other Examples

Advanced

Rogue AP Attacks

Definition

A rogue access point, this covers multiple different attacks such as fake wireless access point (fake WAP) and the evil twin attack, tends to be a hardware device or node on a local area network that can perform this attack.

Access points allow devices and networks to connect via a wireless standard, like Bluetooth and Wi-Fi, if they have the capability to do this. This could be a user’s phone that connects to their router at home, the router being the access point. These access points let connections between devices and the Internet or a network to exist.

Rogue access points will pretend to be innocent access points to perform their attacks. They do this by having a network with the same name as a public one, for example Airport Wi-Fi or Starbucks Wi-Fi. The user can then connect to this network with their device, and the hacker can start to control the way in which the device connects to the Internet.

The hacker can redirect the user to different web pages, ones that they have created for this purpose. By doing this, they can steal information including bank details, logins and more from the user. This is possible as all of the network connection is going to the hacker, so it means that they will get any information inputted by the user.

History

Rogue AP attacks became a popular attack, through means like the evil twin attack mentioned earlier, around the mid-2000s. Around this time, Best Buy and Lowe’s experienced attacks in the same vein as these rogue AP attacks.

One of the first things to be liable to this specific attack was the Windows XP operating system. Released in 2001, XP was very vulnerable to this certain attack. This being as when the system disconnected unexpectedly, the computer using the XP system will automatically try to reconnect to the same network. Because of this, it could be easily taken advantage of.

Hotspotter was a tool created around this time that did this exact attack. Beginning with sending a fake deauthentication packet, looking like it’s coming from the user’s computer. A packet is data that is sent from one place to another over the Internet, so a deauthentication packet will send data that will make the user’s computer no longer recognise the network they were on as authenticated.

After this step, the access point will disconnect from the user’s computer, the attacked coming into the equation. Using their own computer, they will emulate the network they forced the user off of. Since the XP system will try to reconnect automatically, it will authenticate with the hacker’s fake network and will now be connected to a rogue access point.

Protection

Applications?

Other Examples

Advanced

Clickjacking

Definition