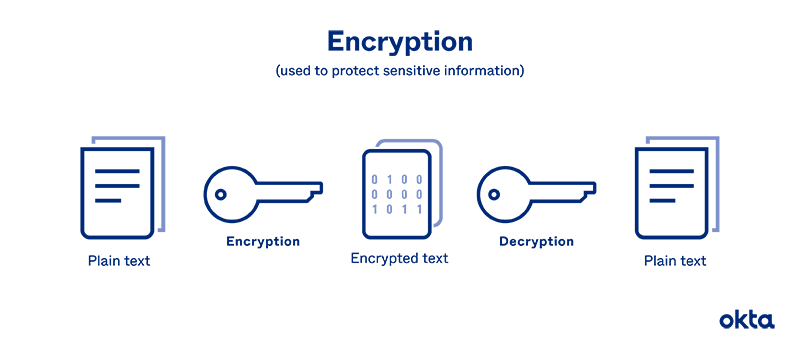
Collaborative Development: Data Base and WIFI encryption and security.

Data Base encryption most often a encryption algorithm is used that will transform the data inside the database from readable into a ciphertext of unreadable text this data can then be decrypted and used as needed if the user has the key that the encryption algorithm generated this is particularly good at keeping your data secure as unlike most security methods like antivirus software this works at the data level meaning even if someone retrieves the data without the specific keys to decrypt it they still won’t be able to view your data.



This means that no matter how secure your password may be no matter how many letters numbers neither how unique it is if the server saves the password in plain text and the data base is then breached due to some vulnerability that has been overlooked it has then gone to waste and now your password will be saved and spread alongside many others on websites therefor it can never be used again.

There are many types of encryption formats that will be used by companies but were going to look at the most used formats which are Advanced Encryption Standard (AES), Blowfish and Triple DES Encryption.

**Advanced Encryption Standard (AES) –** AES is the most common Encryption method used in this list AES is a symmetric key encryption which just means that the key used will both encrypt and decrypt the information.

This encryption type encrypts data in blocks of 128 bits at a time it uses keys of 128, 192 and 256 bits in order to encrypt its data blocks the 128 bit key will encrypt the data in 10 rounds where as the 92 bit will encrypt the data in 12 rounds and then the 256 bit key will encrypt the data in 14 rounds a round consists of transposition , substitution and mixing up plain text as well as many other encryption techniques however all these things are to scramble the data as much as possible to be put through these rounds the into individual blocks in order to encrypt them then after they have been encrypted them will join them all back together to form the final cipher text.

AES is what I would recommend using for most businesses and is what is used the most through out all commercially available encryption methods however this doesn’t mean it has no downsides as one of the most crucial to our small business model is resource intensive and there for it can be slow which can really be brutal for smaller businesses as the cost in order to maintain this security method working at a fast pace would most likely be costly.

**Triple DES Encryption (3DES) –** Triple DES is an encryption method that is modified from the regular DES algorithm that was developed by IBM in the 1970’s they modified it due to the lack of security it provided and with modern computing it just couldn’t keep up there for a modern twist would be needed there for 3DES applies the DES cipher algorithm three times to each data block to ensure that the data block is properly secured.

Although Triple DES is more secure than DES and allows it to compete with modern solutions it is also 3 times slower than DES and there for makes it not time efficient as other modern solutions and has a limited key size of 192 bits which in recent times may not be enough to meet company standards.

The way this method works is that 3 unique keys are generated using an algorithm for key derivation and then the 64-bit plaintext is then subjected to an initial permutation then the plaintext is encrypted three times each time its encrypted it uses a different encryption key each time after this it receives its final permutation which is applied to the out to produce a ciphertext.

**Blowfish –** Blowfish is a symmetric key encryption method that uses 64-bit block cipher that can take a variable length key up to 448 bits from 32 bits it consists of 16 Feistel like iteration and each iteration will operate on a 64-bit block which has been split in to two 32-bit words.

Advantages of blow fish include it’s extremely fast and more efficient than DES and IDEA algorithms its unpatented as well which means it can be used without having a licence making it more accessible to smaller companies it also provides a multitude of tools that can be helpful to the user such as backup functions and secure remote access.

Disadvantages of blow fish are the key schedule takes a long time therefor speed is a problem when changing keys as each key requires preprocessing equivalent to 4 KB to text which one of the reasons it affects the speeds so much also there is a problem with the 64-bit block size being small in comparison to more modern techniques it makes it a lot more susceptible to brute force attacks.

My conclusion to this would be to use Blowfish if we have extremely limited resources due to it being unpatented and it having an efficient data encryption process however with more funding I would have to suggest that you would use AES as it’s standard in many companies for a reason its reliable and allows for the highest level of data encryption other then that its very versatile which allows it to meet most if not all security requirements of the modern day.

# WIFI encryption and security

Wi-Fi encryption and security is essentials for wireless networks that transfer and process sensitive data it is used in order to prevent unauthorized access and data interception attacks that are most commonly used by these hackers are brute force attacks and dictionary attacks another set of really common yet extremely effective methods are packet sniffing and Wi-Fi fishing attacks however continuing on my explanation there are security protocols that have been put in place in order to keep networks secure from many of these malicious attacks such as WEP, WPA, WPA2 and WPA3 these are fundamental when you have important data that you wish to protect.

**WEP – Wired Equivalent Privacy**

This is one of the earliest methods of encryption and was used to secure wireless networks it would encrypt data over a network using a static encryption key however it had quite a few pitfalls which makes it basically unusable if you want to keep your data safe.

1. Weak Key Generation – it used a shared static encryption key for every device on a network and the key generation process is weak and there for leading it to have predictable keys making it easier for unauthorized to cracks them and gain access.
2. Packet injection attacks – It does not provide integrity protection for transmitted data which makes it vulnerable when subjected to packet injection attacks which allows hackers to inject packets which manipulate data or allow their other attacks to run without being noticed.
3. Lack of key management WEP lacks an intricate and customisable key management mechanism making it hard for the user to change or update their encryption key which then increases the chances of a key being compromised the longer its used.

**WPA – Wi-Fi Protected Access**

This was developed in order to replace WEP they wanted to address a fix a lot of the flaws from WEP such as making stronger encryption methods and having dynamic encryption methods allowed and accounting for a lot of the downfalls of WEP making it a definitive improvement however although it fixed some of the issues I was not perfect leading it worked on and improved however it never perfected any of the solutions some of the main pitfalls being.

1. TKIP vulnerabilities WPA used TKIP instead of RC4 like WEP however it still had many vulnerabilities when in came to its key management and encryption process.
2. It also had inadequate encryption methods leading to exploitation which leading to confidential data being compromised.

**WPA2 – Wi-Fi Protected Access 2**

This is the successor of WPA and builds on the previous goals of WPA however using more modern and effective methods in order to provide better protection this method uses a previously described data encryption method called Advanced Encryption Standard (AES) and it provides far greater security measure in comparison to WPA which makes it a very favourable method when it comes to Wi-Fi security however it still has its own set of vulnerabilities which can be exploited.

1. KRACK attacks were one of the main downfalls of WPA2 in which an exploit where in a 4-way handshake process it can reinstall an already in use encryption key which can allow and hacker to decrypt and intercept data that is transmitted over a network.
2. Password cracking is also a big issue due to the weak and easily guessable passwords that are used it can really be a pitfall as they can completely bypass all the work done by the encryption of data by using dictionary attacks and brute force attacks to guess the password and for all intents and purposes with the password the system will treat you as authorised personnel.

**WPA3 – Wi-Fi Protected Access 3**

With WPA 3 it’s the latest generation of Wi-Fi security protocols with the goal to enhance wireless security it also has several improvements over WPA2 some of these improvements are stronger encryption as well as better protection against brute force attacks and increase security for IoT devices with this in mind WPA 3 employs SAE (Simultaneous Authentication of Equals) protocol which is in place of PSK method in WPA 2 this was added to make it more resistant to offline dictionary attacks which is one of the biggest downfalls of WPA 2 as well as having individualized data encryption in order to ensure that if a single device is compromised it will not compromised the entire network however its not without its weaknesses here are some.

1. Hardware support as WPA 3 is a newer standard many devices will not support it which then could cause a lot of companies to have mixed levels of security causing vulnerabilities.
2. Because of it being so new that Is also a major issue as it lacks knowledge surrounding it there are many pitfalls either minute or massive that could be yet to be found meaning that some large companies might not want to change as it could have potential to be insecure in the future.

In conclusion, I believe that It would be best to use WPA2 due to its limitations being well known to others but most by us to therefor we can work around the issues and also be ready for expected attacks rather then putting all our eggs in a more secure WPA3 however having the potential for the metaphorical rug to be pulled under us by an unknown yet massive potential security flaw.

## Grabify Links and Brute-Force Attacks

**Grabify Links -** Grabify Links are generated through grabify Ip loggers service and they allow a user to create a shortened link that will redirect a target URL however when doing so it will capture information about the person who has clicked the link it can log quite a few details about the person who has clicked the link these things being IP address, browser information the type of device that is being used as well as the location of the user these things are very important and this information can be used in malicious ways and therefor security measures need to be taken when dealing the potential of these links being clicked by devices inside a company.

Things that can be done to protect against these types of links are very few as it’s such an efficient method in order to obtain information about a user however there are someways of working around this these include:

* Using VPN’S by using a VPN you can mask your IP address making it unable to access your IP address and therefor will stop it from gathering information such as your location.
* Awareness this isn’t a software tool however educating your staff or yourself on these links can mitigate the number of links you will click considering that you will be able to notice these links in comparison to regular ones making you less susceptible to grabify links.
* URL unshortening services these can be used if you have a link, you believe could be potentially dangerous this will unshorten the link making it readable to the user and easier to determine the legitimacy of the link.
* Anit-Tracking browser extensions can be used which can block tracking script and prevent website from collection user data without your consent.

**Brute force attacks –** A brute force attack is a way of systematically guessing password or encryption keys using an automated script or tools that try a vast number of possible usernames or password until a correct one is found same for guessing encryption keys it will just try a vast combination of potential keys until it finds the right one which will lead to account takeovers and potential data breaches.

Things that can be done to protect against Brute force attacks on our website are:

* CAPTCHA which will then prompt the user for some sort of quiz to prove that there is a user behind the session which if this test is failed deny all access because it will believe you to be a bot, or a computer run script there for being quite effective when brute force attacks are exactly that.
* a two-factor authentication system this will prompt the owner for external information not such as a code that has been sent to there phone as a hacker will not have access to this, they will be unable to get any further thwarting their attack.
* You can also add rate limit login attempts which can be attached to a user or Ip which then restricts the number of times a user can attempt to log in this will make it so a program that would have to try 10’s of thousands of logins would just take an impossible amount of time to continue cracking logins.