Cybersecurity in The Digital Age

How safe is our data?

Rashika Shaw, TechSphere Insights,
April 2025, Volume 1, Issue 4, pp. 30–36.

Introduction

Today, we are living in the digital age, which is also characterised by the widespread use of digital technologies such as the Internet. The internet has transformed the way we work, live, access, and communicate information. Feeling bored? just say hi! to your friend on a Messenger. Want to eat? order food online through Swiggy or Zomato. Don't have the cash to pay, use online payment apps such as Google Pay and PhonePe to make payment, and even when we are looking for trendy, fashionable clothes, we go to e-commerce apps such as Amazon to buy fashionable clothes for ourselves. Things have changed very rapidly; the Internet has given us the privilege to get things at our convenience with just one click. However, alongside these conveniences comes a growing area of concern: the way we share our data online. The global indicator reported that 'the estimated cost of cybercrime' in the cybersecurity market is predicted to increase between 2024 and 2029 by 64.91% consistently. From entering our location, contact details, payment information, and personal data online. We are constantly sharing our data without even realising what if it gets leaked or falls into the wrong hands. The European Union data privacy authorities fined Meta around $ 263 million for the 2018 data breach in which 29 million accounts were compromised. Another example of cyber threats that can also happen without someone sharing their information is E-mail hijacking. Email Hijacking is one way where fraudsters trick users into disclosing confidential information by directing them to any link; this is called a phishing attack in the cyber world. Cybersecurity is the process that is utilised to protect

computer systems, networks, and data from unauthorised access. The present article is going to discuss in depth the types of cybersecurity, its role in securing our data, and the evolving future of Cybersecurity.

The digital footprint we leave behind

Digital footprint refers to the record of all the online activities of a person and their interaction action online. It is the collection of all the digital points that are left behind as a part of someone's digital actions. It can be passive as well as active; passive means the data that is collected by online websites and online services. For example, the online profiles that commercial parties create to analyse the browsing behaviour of consumers to sell the data and showcase ads based on their interests. The active digital footprint means the content created by a person and shared on different digital social media platforms, such as Facebook or Instagram. In the world of cybersecurity, this is also called a cyber footprint. It has been found that, on average, users spend 6 hours of their day on the Internet, while 60% of the total population uses the Internet. Cybercriminals use the digital footprint of the organisation to create convincing phishing emails. For example, sometimes hackers use spoofing techniques to collect the email addresses of any employee and trick them into revealing important login credentials.

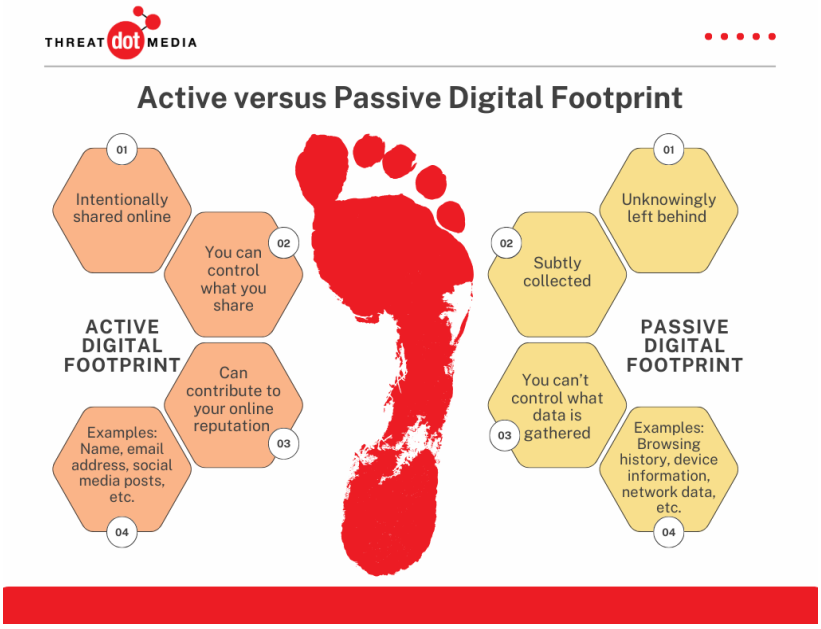

Figure 1: Digital Footprint

Different types of Cybersecurity threats

1) Identity Thefts: In a report published by the Identity Theft Resource Centre, 78% of identity thefts are attributed to job scams and scams in 2023. Identity theft is an illegal act in which a scammer steals important information, including name, email, phone number, or Password, without consent and uses it to obtain financial gain. One example includes unexplained credit card bills or new credit cards issued in a person's name that they did not apply for. Anyone can be a victim of identity theft, but elderly people and children are more vulnerable to this type of attack. This is because, in the case of children, their finances are handled by someone else.

2) Social Engineering Attacks: Spear phishing is a Social engineering attack in which attackers use the activities of a person to trick them. Examples include if a person in a LinkedIn profile shares their interest regarding job roles in social media platforms, the scammers try to manipulate this information to provide fake job offers or click on the link, in which they end up revealing sensitive information that can be used against such as bank account details, OTP. In a report published by IBM, it has been found that phishing is the most common reason for data breaches. The reports of Statista outlined that in a survey report, ½ of the surveyed organisations encountered malware infections on their systems due to spear phishing attacks, while 50% of them witnessed the loss of confidential or sensitive data.

3) Brute Force Attack: In this type of cyber-attack, attackers mainly use a trial-and-error approach to guess the combination of passwords. Examples of this type of attack include recognising weak passwords of any account; it can be perceived as similar to the incident in which hackers try to break the password until they get the right login information. Real examples of this type of attack include in 2016, a popular e-commerce platform, Alibaba, faced this type of attack in which the accounts of 21 million users came at risk. In Brute force attacks, hackers mainly target individuals who use easy passwords or often use the same type of passwords for multiple websites.

4) AI in Hacking: There are instances in which people have shared the sensitive information of their accounts after getting swayed away by the conversation through a virtual assistant. Neural networks in AI are used to recognise passwords. Through the use of Neural networks, hackers are now able to guess passwords easily that look like "passwords". Additionally, sometimes hackers can crack a portion of the password with the help of neural networks.

5) Cyberbullying: Cyberbullying is a type of bullying that takes place over digital devices such as tablets, computers and smartphones. It involves utilising social media, messaging apps, gaming platforms, and online tools to harass, threaten or target another person. One example of cyberbullying is when a person makes a fake profile to impersonate or mock someone. The other example includes posting false or hurtful information about someone else online.

Figure 2: Cyberbullying

Role of cybersecurity in protecting digital data

Cybersecurity is a practice that is designed to keep digital networks, systems, and data safe from unauthorised access. In today's digital world, cybersecurity is just like a lock that keeps your important information can be kept safe and

protected from being stolen, destroyed and misused. We need cybersecurity to protect sensitive personal, financial and business information.

In the above section, we learned about different cyber threats in the digital age and how hackers use basic information to cause financial harm to any individual or big organisation. However, there are some effective cybersecurity methods to ensure our data is secure in the digital age. These are as follows:

Cybersecurity approaches in tackling identity theft

For the cyber-attacks that start through fake emails tricking users into giving away sensitive information, hackers. There are email filters that detect malware, viruses and spam before it lands in users' mailboxes. The report of Statista highlighted that 1 in 6 phishing emails contain dubious attachments to the Department of IT. This phishing not only directs users to download malicious attachments but sometimes also causes fake password reset requests. Thus, not clicking on the link or double-checking before downloading an attachment are ways one can follow on a personal level to avoid becoming a victim of a phishing attack.

Cybersecurity approaches to prevent social engineering

Detecting log-in activity in real-time is one approach that detects anything unusual and reports it immediately. For example, when someone logs into their email account from a different device, the cybersecurity real-time tracking tool tracks this reports this activity to the account holder and asks if the activity was made by them or someone else. When an email account holder gets this message that their account is being accessed by someone in another country, they can either change their password or report it to keep the sensitive information safe.

Cybersecurity Approaches Against Brute Force Attacks

There is no one-size-fits-all solution to the problem of Brute force attacks, but adding multiple levels of security for companies and individuals is the only way to protect systems. We have seen that while making new accounts, we see pop-ups like passwords should be long or add one character, or the password is weak. The goal is to make passwords complex enough to make it difficult to crack by the hackers. Many websites use hashing and salting techniques in which random numbers are added to make passwords difficult to guess, even if the same password is being used in two different places.

Two-factor or Multi-factor authentication (2mfa) is an approach in which an extra layer of security is added to prevent easy access to the financial accounts of the users. This means even if the hacker guesses the password without the second piece of information, it will not be easy for the hacker to log in.

Firewalls are another key defence that spots suspicious behaviour and blocks it from one place.

"Completely Automated Public Turing test (CAPTCHA)", on the other hand, checks whether a login is made by a human or a Bot.

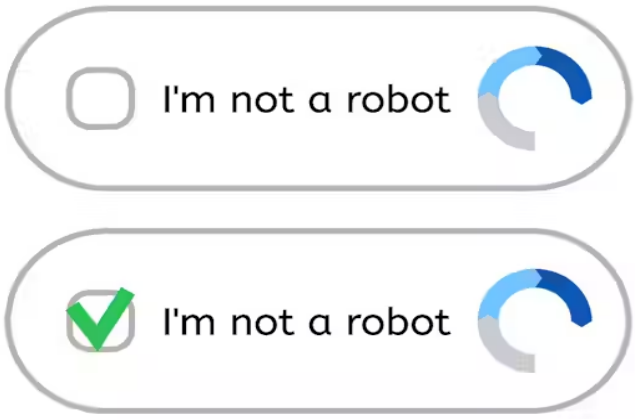

Figure 3: Captcha

AI in cybersecurity

With the nature of cyber threats evolving regularly, the set-it-and-forget-it approach is not going to work anymore. Thus, adaptive defence is an approach that utilises machine learning algorithms to consistently learn from new data and update defence strategies based on evolving types of cyber-attacks. AI adaptive defence approach enables businesses to recognise and stop these attacks through methods such as isolating the system that is under attack, creating effective response plans and applying them, and restoring affected systems through the decryption process.

Cybersecurity approaches to deal with cyberbullying

Reporting and blocking tools are effective features that make it easy for users to report abusive messages or cyberbullying behaviour. Further, the blocking tool enables users to block the bully and limit interaction with the bully. Additionally, in social media platforms such as Instagram and Facebook, there are options such as controlling profile visibility or restricting people from tagging them online. These features help in preventing getting bullied in the virtual world. End-to-end encryption is a method that ensures privacy in conversations between parties, such as WhatsApp. However, WhatsApp also allows flagging selected messages as abusive, even in encrypted chats, by sharing them with moderators.

Are the current cybersecurity practices enough to secure our digital data?

The approaches discussed above definitely improve cybersecurity, but cybercriminals always find new ways to bypass cyber defences. Thus, reflecting upon the question of how safe our data is, the answer is “Our data is safer than before, but never entirely safe”. The technologies, such as Firewalls, encryption, authentication, and AI-powered adaptive defences, significantly make it harder for hackers to succeed. The security of our data significantly depends upon continuous monitoring, regular updates, and awareness of the users.

Securing our digital data in the digital age is not about achieving total immunity from cyberattacks, but practising methods such as thinking before clicking on suspicious links. Additionally, regularly updating software and managing privacy controls on respective apps to improve digital well-being.