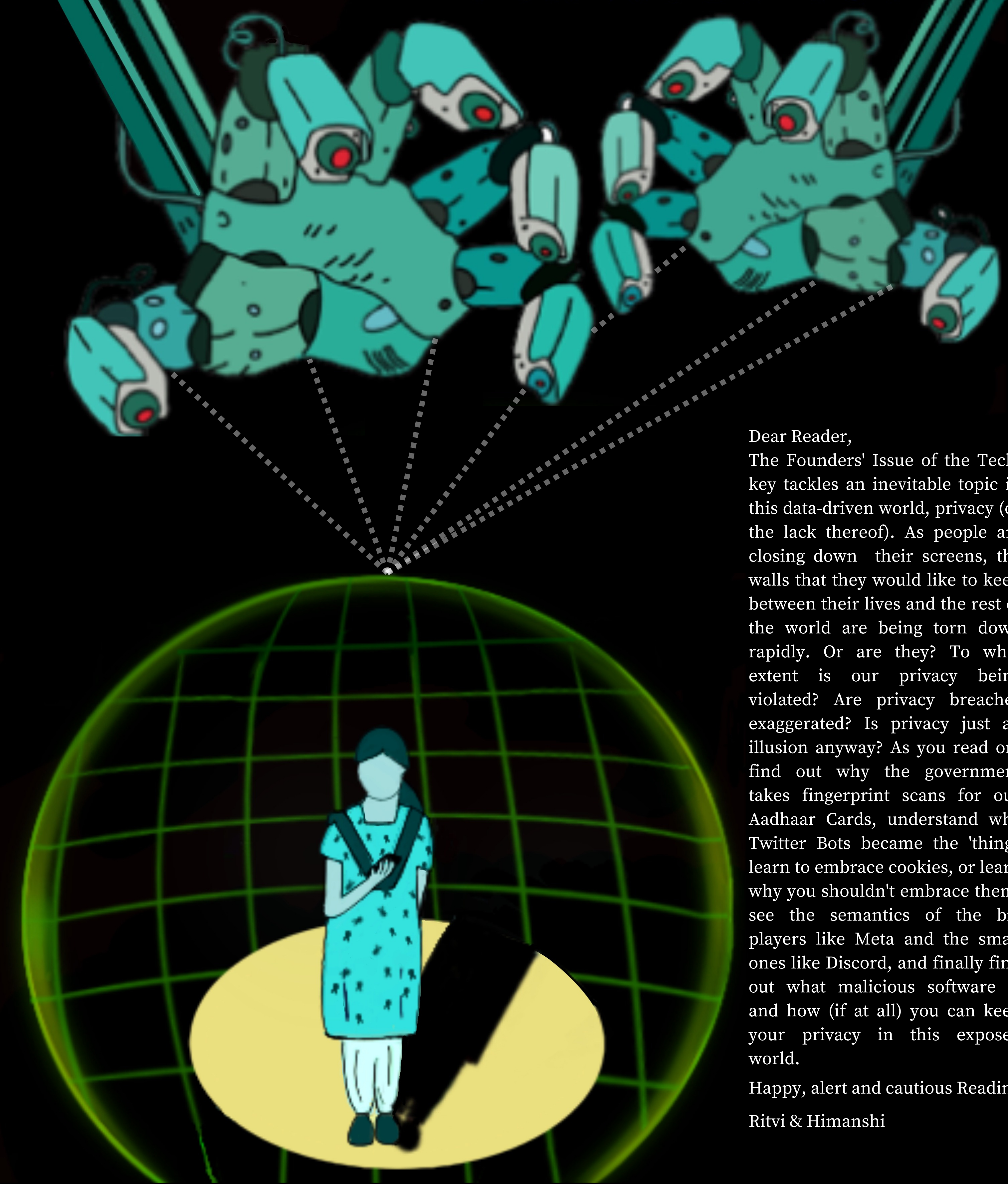
TECHKEY

PRIVACY 101



Dear Reader,
The Founders' Issue of the Techkey tackles an inevitable topic in this data-driven world, privacy (or the lack thereof). As people are closing down their screens, the walls that they would like to keep between their lives and the rest of the world are being torn down rapidly. Or are they? To what extent is our privacy being violated? Are privacy breaches exaggerated? Is privacy just an illusion anyway? As you read on, find out why the government takes fingerprint scans for our Aadhaar Cards, understand why Twitter Bots became the 'thing,' learn to embrace cookies, or learn why you shouldn't embrace them, see the semantics of the big players like Meta and the small ones like Discord, and finally find out what malicious software is and how (if at all) you can keep your privacy in this exposed world.

Happy, alert and cautious Reading!

Ritvi & Himanshi

AADHAAR CARDS FOR FORENSICS

ETHICAL OR A PRIVACY BREACH?

Illustration by Prisha Kejriwal

The Unique Identification Authority of India (UIDAI) is an organisation tasked with collecting demographic and biometric data on the nation's citizens, storing the information in a large database, and issuing each citizen a 12-digit unique identity number known as an Aadhaar. The Aadhaar Act, of 2016, established UIDAI and seeks to provide the Aadhaar unique identification number initiative legal support.

The UIDAI recently notified the Delhi High Court that fingerprints discovered at a crime scene cannot be compared to the Aadhaar database to identify perpetrators. It claims that the Aadhaar Act of 2016 forbids the use of fingerprints to identify offenders.

According to Section 29 of the act, no basic biometric data gathered per the Aadhaar Act 2016 may be disclosed to anybody or used for any purpose other than the creation of Aadhaar numbers and legal authentication. Technology also bars officials from using it in criminal identification, as the UIDAI does not collect biometric information based on technology or procedures suitable for forensic purposes.

According to Section 33 of the Aadhaar Act, 2016, identity information or authentication records may be revealed with a High Court or Supreme Court judge's decision and after the UIDAI and the Aadhaar bearer have been given a chance to be heard. However, “core biometric information shall not be disclosed under this subsection”.

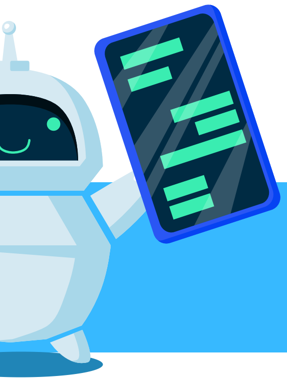
Now is this advisory protecting criminal rights or slowing down an already inefficient police processing system?

We live in a country plagued by overpopulation and recession. The only standardised mode of identification we have is Aadhaar Card. It is the only thing the entire population of 138 crores has. Then comes our backward policing system fuelled by low funds, corruption, and bureaucracy. If the Aadhaar database can help the productivity of the Indian Police Service, doesn’t our need for justice outway a criminal’s right to privacy?

-Tahira Kaur Dhillon
Sc-A

THE BATTLE OF TWITTER BOTS

#ELON MUSK



twitter

Have you even come across a twitter account making claims that seem unbelievable? Or accounts that have a lot more retweet activity compared to other active accounts?

Well, you have probably come across a twitter bot.

So, what exactly are these accounts that have the Musk-twitter deal dangling over headlines for over a year?

Twitter bots are accounts that are automated by bot softwares. They use the twitter API to interact with users. These bots can perform specific tasks such as liking tweets or retweeting on a large scale. While these accounts improve the efficiency of many tasks such as spreading information or weather broadcasting, they also do equal harm. By simply liking or commenting on tweets on a large scale, they possess the ability to bully, persuade or brainwash the masses into beliefs built on false information. In simpler words, they keep the ability to spam the general public with heavy misinformation that can lead to serious problems in the real world.

Cybercriminals can also use such accounts to spread malware (virus) among users.

Further, they are used to spread political propaganda and even influence elections.

Found on twitter since the founding of the application, these bots are so impactful that they are making billionaire Elon Musk reconsider his purchase of the social media platform. On April 14 2022, Musk offered a deal of 44 billion dollars for what he believed would 'unlock the app's extraordinary potential'. However, a 44 billion deal does not happen overnight. When Musk claimed that he 'looks forward to working with twitter', he drew his attention to the increasing spam and bot accounts on the platform. His decision to put the deal on hold till twitter proves the number of bots to be less than 5%, was followed by heavy criticism of the company's action to curb the rising scammers.

As Elon Musk continues to pressurise twitter to look into their bot policy, we must realise that this automated software is not going away anytime soon. In a world that has given way to the era of artificial intelligence, we might as well learn to dwell among these bots.

-Bhavya Sangal
PreSc-A

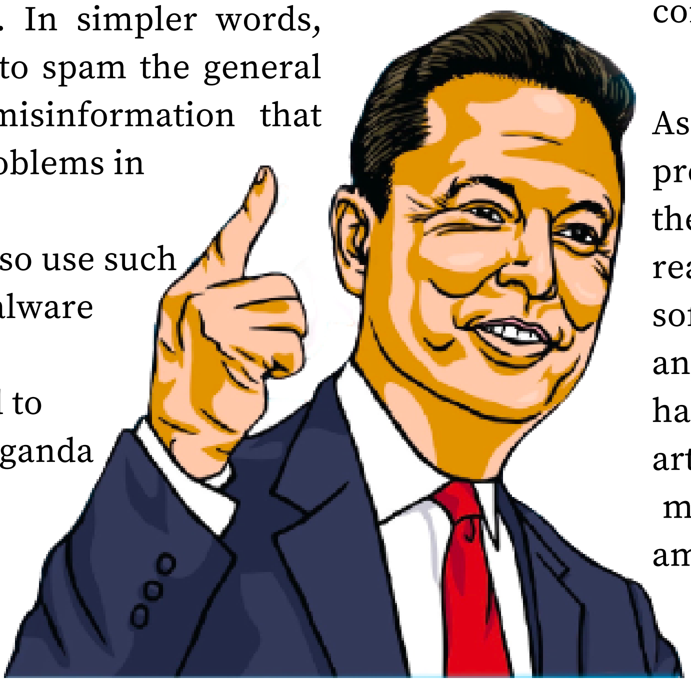


Illustration by Vanshika Gupta

Cookies: Poison in the Recipe?

Illustration by Nimrat Grewal

What do advertisers and Sesame Street monsters have in common?
They love cookies!

“This website uses cookies to give you the best experience, accept all?”

Are you someone who just blindly accepts these cookies, thinking you will truly get the best experience possible? Don’t lie, you know you do. Don’t worry, you’re not alone, I was someone with the biggest cookie jar, until Arshiya asked me to write an article and now, I hope that this article will make you think twice before repeating my mistake.

The main function of a cookie is to remember your activity on the website. It can be helpful for things like a preferred language or a shopping cart. For a site you frequently visit, its absence would make the website as confusing as navigating through a labyrinth. The are different types of cookies too - first-party, second-party and third-party cookies. While first-party cookies only track the user on that particular site, a third-party cookie can track the user on multiple domains, invading any sense left of privacy in this constant world of surveillance.

Cookie poisoning emerged as something that sent us back to reality, forcing us to face the fact that this digital age is not utopian. As the population of the cyber world has increased, so have the attackers. Cookie poisoning is an attack strategy in which the attacker alters, forges, hijacks, or otherwise "poisons" a valid cookie sent back to a server to steal data, bypass security, or both.

But even without cookie poisoning, the entire practice of collecting the user’s activity is flawed. It has so many loopholes, it’s practically Swiss cheese. This is where the concept of data management emerges. Essentially, data management is what an organization chooses to do with the data collected by the cookies. This data can be used to make better business decisions, or it can be sold to advertisers. Oh, and by the way, not all cookies are consensual. Back in 2020, France fined Google 120 and Amazon 42 million USD. Under European law, users should be distinctly informed before the cookies can collect data. And to top it all, these cookies were non-essential. The CNIL, an administrative regulatory body whose mission is to ensure that data privacy law is applied to the collection, storage, and use of personal data, even when the user deactivated personalised advertising on Google, it only worked partially as an advertising cookie always remained stored in the device and continued to process the situation.

Do you now understand how grave the situation is, dear reader? Any activity online could be processed. It’s like George Orwell’s 1984, ‘Big Brother is watching you’. So the next time you willingly accept non-essential cookies, just imagine some marketer standing behind you, looking over your shoulder, and noting down your entire personality. Your data is precious, so treat it like what it is, magic. And you, a magician, should never reveal your secret.

-Paridhi Saboo
A1-A

THE METAVERSE OF MISINTERPRETATION

AN EFFORT TOWARDS PERFECTION

Recently, Meta unfurled a new set of terms of service, its focus being a new privacy policy, but how does it really affect us? Privacy policies are integral to companies and to consumers because they guarantee respect for privacy while also upholding trust for the company.

Meta (earlier known as Facebook), a California-based corporation that was founded in 2004 is now a social media giant, with several messenger sites under its wing, namely WhatsApp and Instagram, among others. Over the past few years, Meta has come under fire many a time due to users' allegations of selling their users' data to 3rd party companies without explicit mention.

Therefore, finally on 26th July 2022, Meta released an updated term of service which predominantly aimed at streamlining the technical and legal terms used. This move was a long awaited one with Meta facing backlash many times over the years. In 2012, Instagram rolled out modified terms of service. Due to lack of understanding of the technical jargon, users misinterpreted this to be an attempt to sell their images and related data.

Illustration by Nimrat Grewal

The company had to retract said old policy and amend it to make it more user friendly. This 2022 amendment was also done to combat criticism from policy-makers and privacy experts. It mainly aims at helping users understand how the company uses and shares the data. However, the amended policy only applies to a subset of ventures, such as Facebook, Instagram, and Messenger.

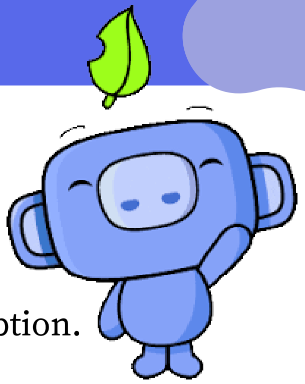
This change is accompanied with 'Privacy Centre,' a feature where you can access the privacy policy and new tailored settings. Some of these are restricting the users who can see your posts and what type of adverts you would like to view. When a user now selects an "audience" to view their post, the change will be applied to all new posts uploaded to Facebook and Instagram. Now one raises the doubt whether everyone needs to comply to these policies or not. The update does not urge users to consent to the new Policy and does not restrict access to the site in case of denial.

This change has come amidst chaos for the company and is viewed by a multitude to be a genuine attempt at improving the reputation of the conglomerate. Concerning metrics released by the company paint a rather ugly picture for its future, with Facebook losing active users every day and incurring a 71-billion-dollar loss this year. Was it to restore a fall from grace, or perhaps an attempt to boost revenue?

-Tvisha Mahajan and Arushi Vohra
A1s

- TECHSPLAINED -

Discord

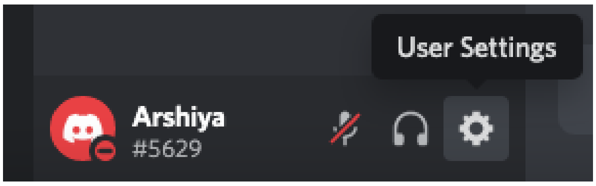


If you're part of the gaming community online or are someone who likes to surf the internet daily, you would've come across the Silicon Valley fashion application, **Discord**.

It is a chat service which focuses on user-friendliness and minimal game disruption. On Discord, users can communicate via text, images, videos, calls and even screen shares – either privately or in public 'servers.' And if you invest into their premium service namely 'Nitro' you can even avail the option to play games including Poker Night, Chess In The Park, Doodle Crew, Word Snacks, Letter Tile, Spellcast, and Watch Together with other Nitro users, a small part of the exceptionally convenient Nitro perks.

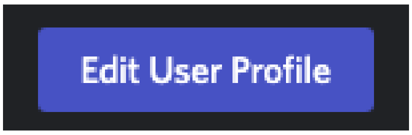
In today's article on how to navigate on discord (press ctrl/cmd + K on your discord screen), we're going to **learn how to set up a profile** and **join public servers**.

Setting-up a Discord Profile

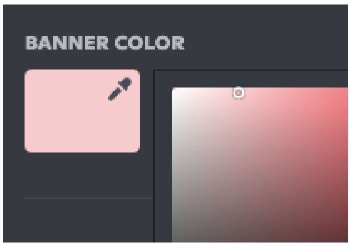


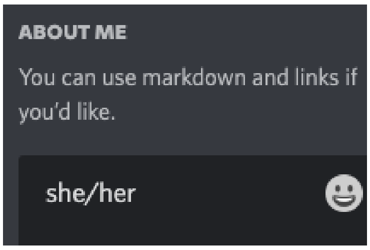
Go to the bottom left corner of your discord screen where you see your name and click on the settings option. Discord provides users the flexibility to choose any name that they want by designing a unique tag for them.

On clicking the settings option, you'll see a **'My Account'** screen. From here you can change your linked email and phone number as well as change your name by directly clicking on the respective options.



Further if you want to change your profile picture, you need to click on **'Edit User Profile'** where just by hovering over the profile picture you get an option to change it. If you have Nitro, you can give yourself a cool banner too! But otherwise you can fill any color you want into your banner and give yourself a meaningful **'About Me'**. You can also preview these changes on the preview panel on the right.





ABOUT ME

You can use markdown and links if you'd like.

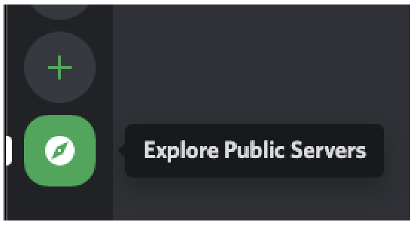
she/her

Joining Public Servers

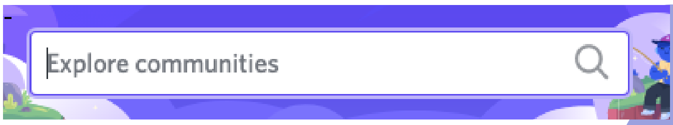
Now that you have successfully built your discord profile, get ready to meet some new interesting people on the internet or maybe join your favourite artists' fanclub server.

Discord offers users a platform where they can find public servers and join them based on their choice.

On the left panel under **'Add a Server'** there's an option to **'Explore Public Servers'**



After doing so you can either pick a server from selecting a category on the left panel or search up keywords to enter your favourite community from here



site link: https://discord.com

-Arshiya Sharma
PreSc-A

MALICIOUS SOFTWARES

PHISHING ATTACK

Phishing is when an attacker tries to trick you into clicking a malicious link that downloads malware or redirects you to a questionable website. It may occur when an attacker posing as a trusted entity tricks a victim into opening an email or an instant/text message.

DDOS ATTACK

A distributed denial of service attack is a cyber-attack against a specific network or server aimed at flooding the target with constant traffic to disrupt normal operations.

In a DDoS attack, cybercriminals exploit the normal behaviour between network devices and servers. Attackers focus on edge network devices (routers, switches, etc.) rather than individual servers.

MAN IN THE MIDDLE ATTACK

The Man-in-the-Middle (MiTM) attack is a type of cyberattack in which an attacker underhandedly intercepts and forwards messages between two parties he believes are communicating directly with each other.

A MITM attack occurs when a hacker takes control of a Wi-Fi network or establishes a free, unencrypted Wi-Fi connection. In this way, hackers can intercept data between the two parties.

SQL INJECTION ATTACK

Structured Query Language Injection is a technique used to exploit user data about web page input by injecting SQL commands as statements.

SQL injection is performed using a structured query that triggers the desired response. This answer is essential for an attacker to understand your database architecture and access your application's protected information.

MALWARE ATTACKS

Malware attacks are common cyberattacks in which malware (usually malicious software) performs unauthorised actions on a victim's system. Malware can infect PCs, smartphones, tablets, servers, and even devices (basically any device with processing power). It can affect us by tricking us into clicking or installing a program that could download viruses into our system.

PREVENTION

Antiviruses like Kaspersky, Norton, and McAfee are programs which, on installing, detect and protect that particular device or network from malware and threats. All tablets, phones, smart watches, printers, and even ATMs connected to a network are endpoints. They act as entrances for malware and other security breaches. Securing these endpoints before they get infected is smarter than recovering your data after it is infected, 'Prevention is better than cure'.

Endpoint security is one of the smartest, cheap, and most effective ways to safeguard your data. Protecting and scanning each file that an endpoint uploads to a network helps secure your data from cyberattacks from the entrance of any malware. Zero trust policy, as the name suggests, advises users to not trust any email, call, or any other form of contact that encourages the user to give out any personal information without verifying the source. Creating strong passwords reduces the chances of one's password being predictable or guessed. Enabling two-factor authentication spreads out an additional layer of security that helps protect your data even if your password is hacked. These measures are easily implementable and will safeguard your data over a long period.

-Akshita Goyal and Vaishnavi Agarwal
A2s

GAME OVER

CREDITS

EDITORS-IN-CHIEF
RITVI AGARWAL AND HIMANSHI GUPTA

SENIOR EDITOR
ARSHIYA SHARMA

ASSISTANT EDITOR
SHAMBHAVI CHANDRA

EDITORIAL BOARD
BIDISHA DAM
KEYA AGGARWAL
NANDINI JALAN
VANSHIKA AGARWAL

ILLUSTRATORS
PRISHA KEJRIWAL
VANSHIKA GUPTA
NIMRAT GREWAL

TEACHER-IN-CHARGE
MS. SAPNA SHARMA

SPECIAL THANKS
MS.SHEFALI THAPLIYAL
MS.MAMTA GOVIL
MS.KAMAL HANDA

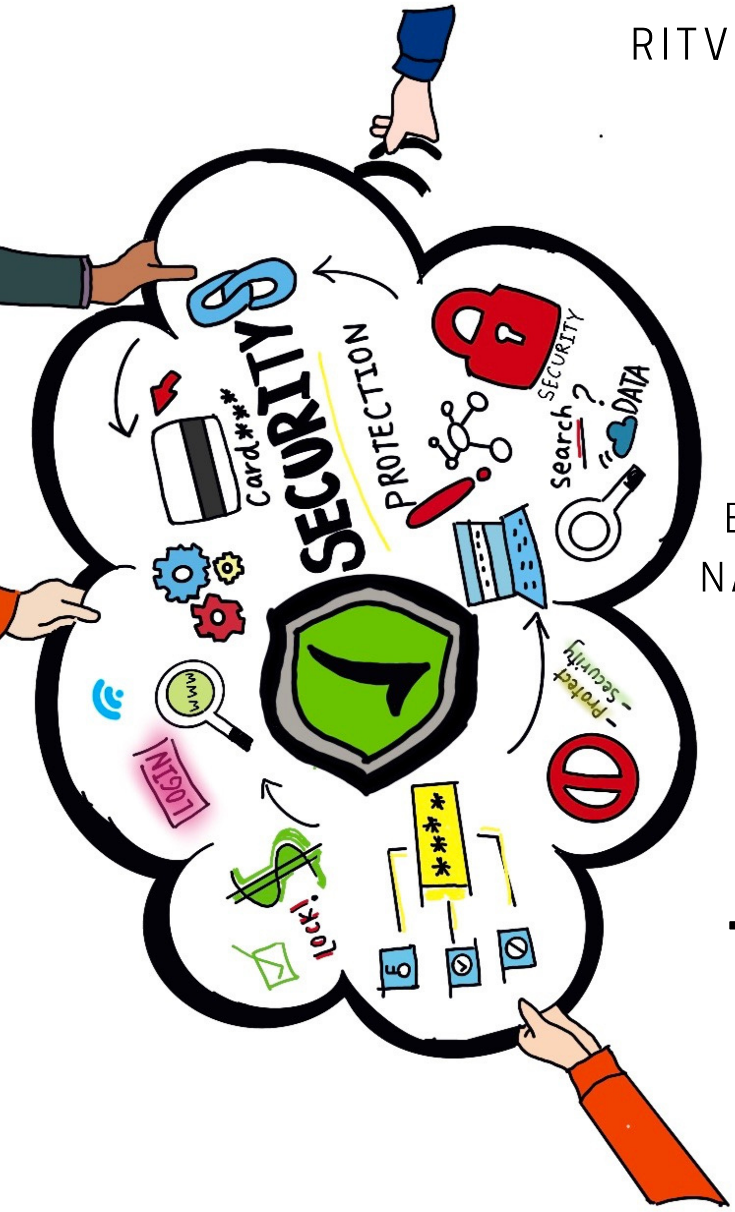


Illustration by Vanshika Gupta

PROTIPS

'haveibeenpwned.com'

Have I Been Pwned allows you to search across multiple data breaches to see if your email address or phone number has been compromised. To date, HIBP has been around for almost a decade, and it has only proven itself to be an essential tool for everyday internet users, governments, and organizations alike. All you have to do is, go to the site and enter your mail. It then tells you if your data has been leaked or fallen trap to data breaches. You can then review your accounts and change your passwords and details accordingly.

'psafe.com/dfndr-lab'

Psafe's link checker is a free tool that detects malicious URLs including malware, scam and phishing links to protect you from any suspicious websites. So if you're ever in doubt of a website that doesn't look like it's upto any good, it's no harm to search up psafe link checker and secure yourself.