OCT-DEC 2022

VOLUME 1 NO 3

{CODE IT}

https://vaguefoundation.com

THEME: CYBER SECURITY

EDITORIAL

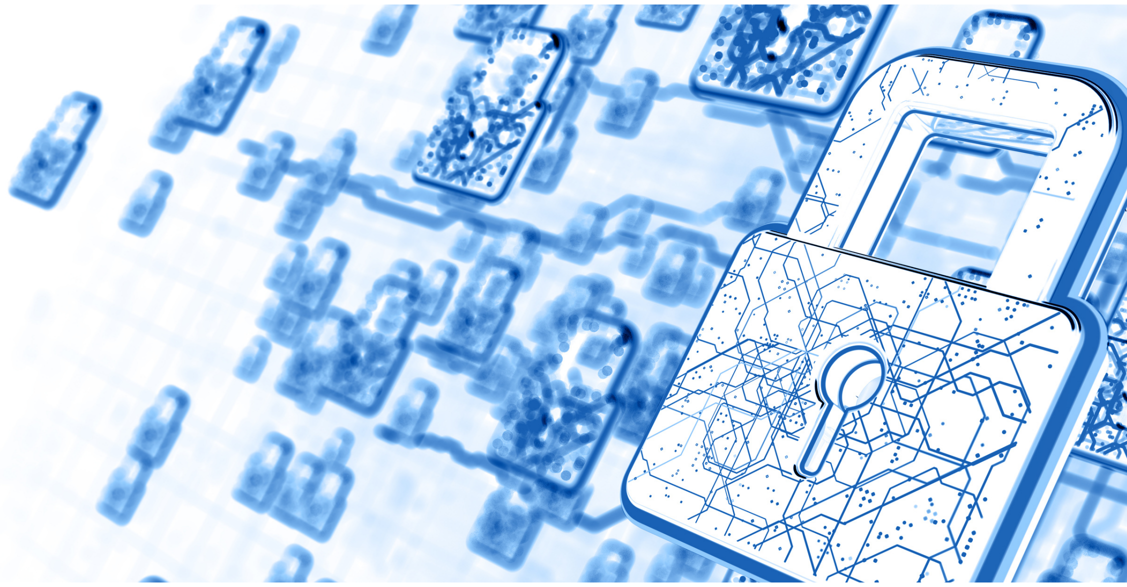
Cybersecurity is one of the most significant challenges of the contemporary world, due to both the complexity of information systems and the societies they support. Security is of especially high importance for systems that govern large-scale systems with far-reaching physical effects, such as power distribution, elections, and finance.

Since the Internet's arrival and with the digital transformation initiated in recent years, the notion of cybersecurity has become a familiar subject in both our professional and personal lives. Cybersecurity and cyber threats have been consistently present for the last 50 years of technological change.

Vast career opportunities in the field of Cyber Security are there for passionate students, where they can be in a challenging and keep-changing environment to save human wealth and lives.

Happy Coding!

CONTENTS



GUEST ARTICLE

by ***Ms. Shivani Acharya***

The definition of cyber security is; protecting networks, data, programs, and other information from unattended or unauthorized access, change, or destruction. Around the globe nowadays, cyber security is very vital because of the threat of cyber-attacks. The cyber security software market is a multimillion business overgrowing at 9.8% per annum and is likely to reach USD 260 billion by 2026. These mammoth figures indicate the gravity of cyber-attack threats and the importance of cyber security. Many companies develop software for data protection. The main task of the software developed by the companies is to protect the data in their system. Not only does cyber security helps to secure information, but it also protects it from a virus attack. India is one of the countries with the highest number of internet users, after the USA and China.

Cyberthreats and Cybercrime

Cyber threats can be classified into two major types: Cybercrime, which happens against an individual, or corporate, etc., and Cyber-warfare, which happens against a state.

Cybercrime is the abuse of cyberspace such as cell phones, computers, the internet or other technical devices, etc. By using numerous codes and software in cyberspace, cyber attackers can commit cybercrime. Through the use of malware, the attackers exploit the weakness in the hardware and software design. Hacking is an ordinary way of penetrating the defenses of protected computer systems and disrupting their functioning.

Cybercrimes may occur directly by targeting computers and spreading computer viruses or by using Denial of service attacks, which is an attempt to make a network or machine unavailable to its projected users. Software, malware is used to gain access to a private computer, gather sensitive information, or disrupt computer operation.

Do's and Don'ts

The easiest thing that an individual can do to beef up their security and relax knowing their data is safe is to change their passwords. Many password management tools can be used to keep track of everything for an individual as these applications help them use unique, secure passwords for every website one needs and keep track of all the passwords.

To add extra security to logins, one can enable two-factor authentication as the extra layer of security makes it harder for an attacker to get into someone’s account. Keeping one’s software up to date is also a way to prevent cyber-attacks.

What Schools can do?

During the pandemic, schools have quickly become one of the favored targets of cyber criminals. This doesn't come as a surprise, as many areas are limited by budgets and have had to rush their adoption of new digital technologies, increasing the risk of a successful breach or cyber attack. In this new normal, school leaders must learn how to take appropriate actions against these threats to ensure the safety of students, staff, parents, and administrators.

When the network is unavailable, as with a successful Distributed Denial of Service (DDoS) attack, schools lose precious instructional hours. Teachers who are prepared to use technology in the classroom need to take time to find and fall back on non-digital resources.

Breached student records may be maliciously modified, negatively impacting students' future college applications or employment. When student identities are stolen during elementary or secondary school years, no one may be wiser until the students apply for college financial aid. When leaders don't take cyber security for schools seriously, these situations are more likely to occur.

Schools also need to protect students' locations and addresses. You don't want that information out in the wrong hands where it could be a safety concern, especially if you have students who come from abusive households, domestic violence situations, or are in witness protection programs.

Not only do you have to be secure in handling digital records, you must also ensure that the vendors who handle student records are following proper security protocols.

Ms. Shivani Acharya *is the Principal of Radhika EduCare School, Jamnagar. She is a renowned educator and having a vast experience in leading schools. She keeps updating herself and motivating mentors with her kind and cooperative gestures.*

resshivaniacharya@gmail.com

CREATIVES

Cyber Security by Ms. Maulie Abraham

In the current world that is run by technology and network connections, it is crucial to know what cybersecurity is and to be able to use it effectively. Systems, important files, data, and other important virtual things are at risk if there is no security to protect them.

Cyber security is the protection of internet-connected systems such as hardware, software, and data from cyber threats. The practice is used by individuals and enterprises to protect against unauthorized access to data centers and other computerized systems.

Benefits

The benefits of implementing and maintaining cyber security practices include:

- Business protection against cyber-attacks and data breaches.
- Protection for data and networks.
- Prevention of unauthorized user access.
- Improved recovery time after a breach.
- Protection for end users and endpoint devices.

Types of Cybersecurity Threats

The process of keeping up with new technologies, security trends and threat intelligence is a challenging task. It is necessary in order to protect information and other assets from cyber threats, which take many forms. Types of cyber threats include:

- **Malware** is a form of malicious software in which any file or program can be used to harm a computer user. This includes worms, viruses, Trojans, and spyware.
- **Ransomware** is an attacker that locks the victim's computer system files -- typically through encryption -- and demands payment to decrypt and unlock them.
- **Phishing** is a form of social engineering where fraudulent email or text messages that resemble those from reputable or known sources are sent
- ·And a few more…

Challenges

Cyber security is continually challenged by hackers, data loss, privacy, risk management, and changing cyber security strategies. The number of cyber-attacks is not expected to decrease in the near future. As new technologies emerge, and as technology is used in new or different ways, new attack avenues are developed. Keeping up with these frequent changes and advances in attacks, as well as updating practices to protect against them, can be challenging.

Vendors and Tools

Vendors in the cyber security field typically offer a variety of security products and services. Common security tools and systems include Firewalls, Endpoint protection, Antimalware, Data loss prevention (DLP), Encryption tools etc.

Courtesy: shorturl.at/lmpY7, shorturl.at/mZ156

***Ms. Maulie Abraham** is a mentor at Radhika EduCare School, Jamnagar. She is always energetic and ready to adapt any challenges. She is also the Coordinator for Coding activities at RES.*

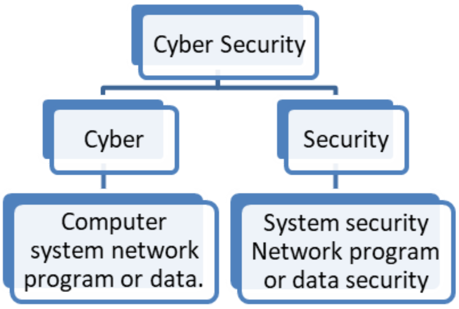
resmaulieabraham@gmail.com

CREATIVES

Cyber Security** by **Mr. Nirav Panara

What is Cyber Security?

“Cyber security is the protection of internet-connected system including hardware, software & program or data from cyber attacks”


Cyber Security
Cyber
Security
Computer system network program or data.
System security Network program or data security

I usually visit a website called www.shoppingcart.com and I have the details of mine like my email address, and debit and credit card details saved on the website to enable a faster and hassle-free shopping experience. The required information is stored on a server. One day I received an email that stated my eligibility for a special discount voucher from shoppingcart.com. In order to receive the coupon code I was asked to fill in the shoppingcart.com account credentials. This didn’t seem fishy to me at the time as I thought it was just an account verification step, but little did I realize the danger I would be facing. I was knocked off my feet when a substantial amount of money was wiped off my account. How do you think this happened? Well, yes the email I received was fake and the shoppingcart.com account witnessed unauthorized access from a third party. This type of attack is known as CYBER ATTACK and a person who carries it out is called a HACKER. I have prevented this attacked indeed; I could have with help of cyber security!

Types of Cyber Attacks

Cyber security involves techniques that help in securing various digital components, networks, data, and computer systems from unauthorized digital access. There are multiple ways to implement cyber security depending upon the kind of network you are connected to and any type of cyber attack you are prone to. So let’s take a look at various cyber attacks that I could have been exposed to one of the most common types of cyber attacks is a malware attack like Trojan, adware and spyware to name of few had downloaded any suspicious attachments online. My system could have gotten corrupted by certain malicious viruses embedded within the attachments.

Next is a **phishing attack.** The type of cyber attack which I experienced, here the hacker usually sends fraudulent emails which appear to be coming from a legitimate source. This is done to install malware or to steal sensitive data like credit card information and login credentials.

Another type of attack is a Man-in-the-middle attack. Here the hacker gains the access to information path between the device and the website's server. The hacker’s computer takes over an IP address by doing so the communication line between the person and the website is securely intercepted. This uncommonly happens with unsecured Wi-Fi networks and also through malware.

A **password attack** is one of the easiest ways to attack a system. Here passwords could have been cracked by using either common passwords or trying all possible alphabetical combinations.

To prevent future cyber attacks we sought to implement a few cyber security practices. First, install a firewall as the name suggests, it is a virtual wall between the user’s computer and the internet. Firewalls filter the incoming and outgoing traffic from your device to safeguard your network and can either be software applications or Hardware reinforcements.

Secondly, implemented honey pots just like flowers attract bees, dummy computer systems called honey pots are used to attack attackers. These systems are made to look vulnerable in order to deceive attackers and this in turn defends their

CREATIVES

real system. In addition to this users should also use unique alphanumeric passwords, and antivirus software and started avoiding emails from unknown senders.

Cyber attacks are not just confined to individuals but also to public and private organizations. The Cyber attacks carried out in such places and more deadly and they result in colossal losses motives for such attacks are many starting from tampering with crucial data to monetary gains. Let's have look at a few cyber attacks that companies are subjected to by various public sector organizations and large corporations face the advanced persistent threat APT. In this form of attack, hackers gained access to networks for a prolonged period. Companies also witnessed denial-of-service attacks where networks are flooded with traffic which in turn leaves legitimate service requests, a variant of this is the distributed denial-of-service DDoS attack when multiple systems are used to launch the attack when a hacker manipulates a standard SQL query in a database driven website, it is known as SQL injection attack by doing so hackers can view and delete tables from the database.

Career in Cyber Security

Amidst a plethora of cyber attacks, it is indeed a challenge for organizations with several networks and servers to ensure complete security. This is not an easy task and to help with this cyber security professionals are hired to work on identifying cyber threats and securing the company's network. There are multiple java roles in the field of cyber security. If hacking fascinates you then the role of an ethical hacker is something to be explored. Such professionals try to expand networks vulnerabilities just like how a hacker would do but only to identify those vulnerabilities and resolve them for protection against an actual cyber attack if you are looking to design a robust security structure then the role of security architecture is more APT a chief information security officer C ISO plays a crucial role in enterprise security and is entrusted with the overall safety of the information in the organization.

Source: Various Youtube Videos

__Mr. Nirav Panara__ is a mentor at Radhika Classes, Jamnagar. He is always very cooperative and supportive. Other than mentoring, he is passionate about anchoring and providing his service of anchoring professionally.

✉ ***nirspanara@gmail.com***

CREATIVES

Cyber Security** by **Hajar Dhrolia

What is cyber security? How can we prevent it? And what harm can it do to us? Cyber security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It's also known as information technology security or electronic information security as it protects our personal information from cyber threats. The global cyber threat continues to evolve at a rapid pace, with a rising number of data breaches each year. A report by Risk Based Security revealed that a shocking 7.9 billion records have been exposed by data breaches in the first nine months of 2019 alone. This figure is more than double (112%) the number of records exposed in the same period in 2018.

Medical services, retailers, and public entities experienced the most breaches, with malicious criminals responsible for most incidents. Some of these sectors are more appealing to cyber criminals because they collect financial and medical data, but all businesses that use networks can be targeted for customer data, corporate espionage, or customer attacks.

Cybersecurity Threats

There are many types of cyber threats as follows;

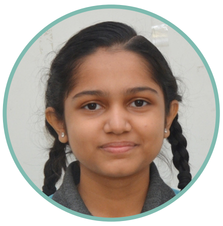
- Virus: A self-replicating program that attaches itself to clean files and spreads throughout a computer system, infecting files with malicious code.
- Trojans: A type of malware that is disguised as legitimate software. Cybercriminals trick users into uploading Trojans onto their computers where they cause damage or collect data.'
- Spyware: A program that secretly records what a user does, so that cybercriminals can make use of this information. For example, spyware could capture credit card details.
- Ransomware: Malware that locks down a user's files and data, with the threat of erasing it unless a ransom is paid.
- Adware: Advertising software that can be used to spread malware.
- Botnets: Networks of malware-infected computers that cybercriminals use to perform tasks online without the user's permission.

Recent Cyberthreats:

- Romance scams: In February 2020, the FBI warned U.S. citizens to be aware of confidence fraud that cyber criminals commit using dating sites, chat rooms, and apps.
- Emotet malware: In late 2019, The Australian Cyber Security Centre warned national organizations about a widespread global cyber threat from Emotet malware.

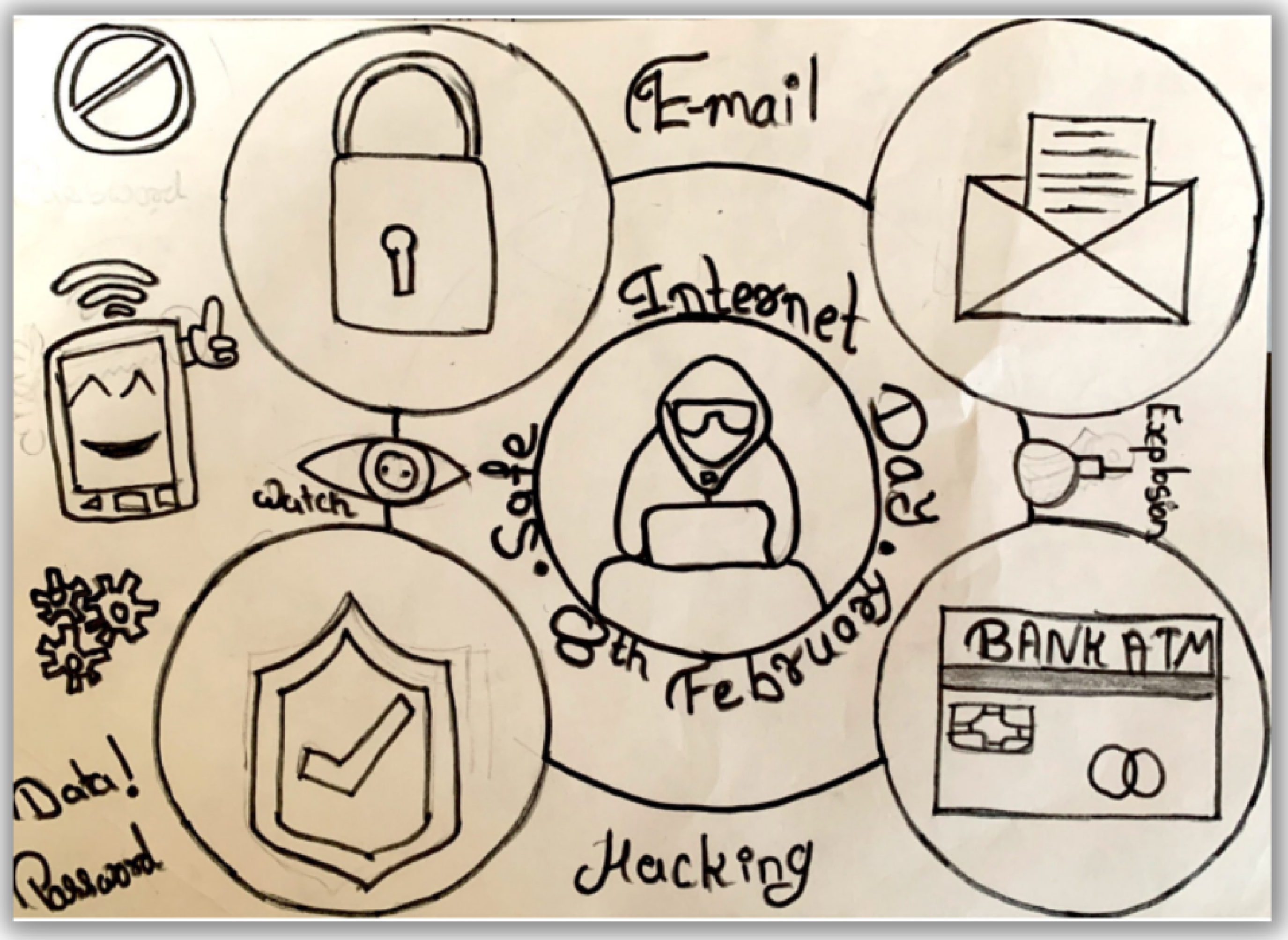
What to do?

- Updating your software and operating system.
- Using anti-virus software.
- Make strong passwords.
- Don't open email attachments from unknown senders.
- Do not click on links in emails from unknown senders or unfamiliar websites.
- Avoid using unsecured WiFi networks in public places.



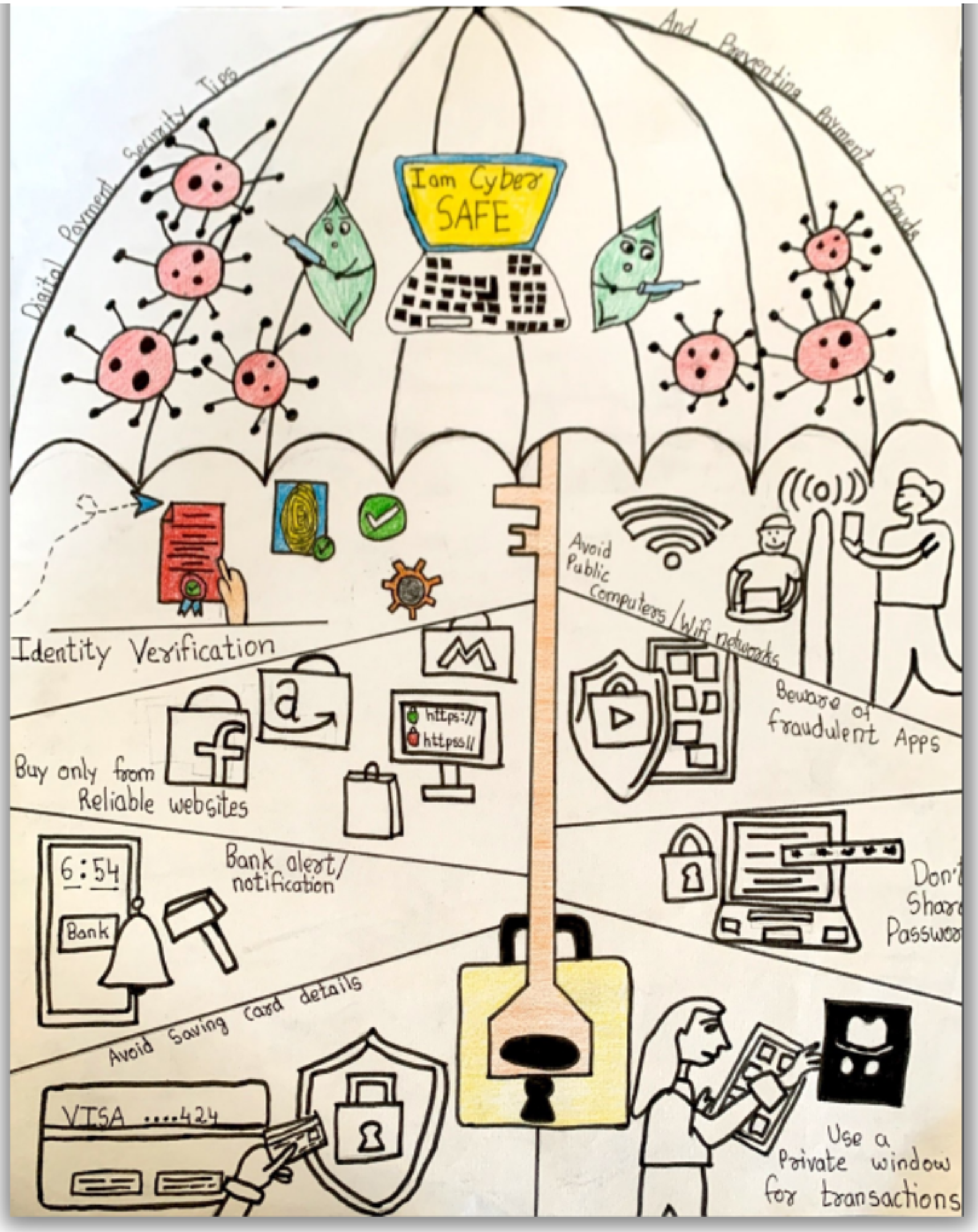
***Ms. Hajar Dhrolia** is a student of Grade-X at Radhika EduCare School, Jamnagar. Along with studies, she is also active in co-curricular and extra-curricular activities of the School.*

CREATIVES



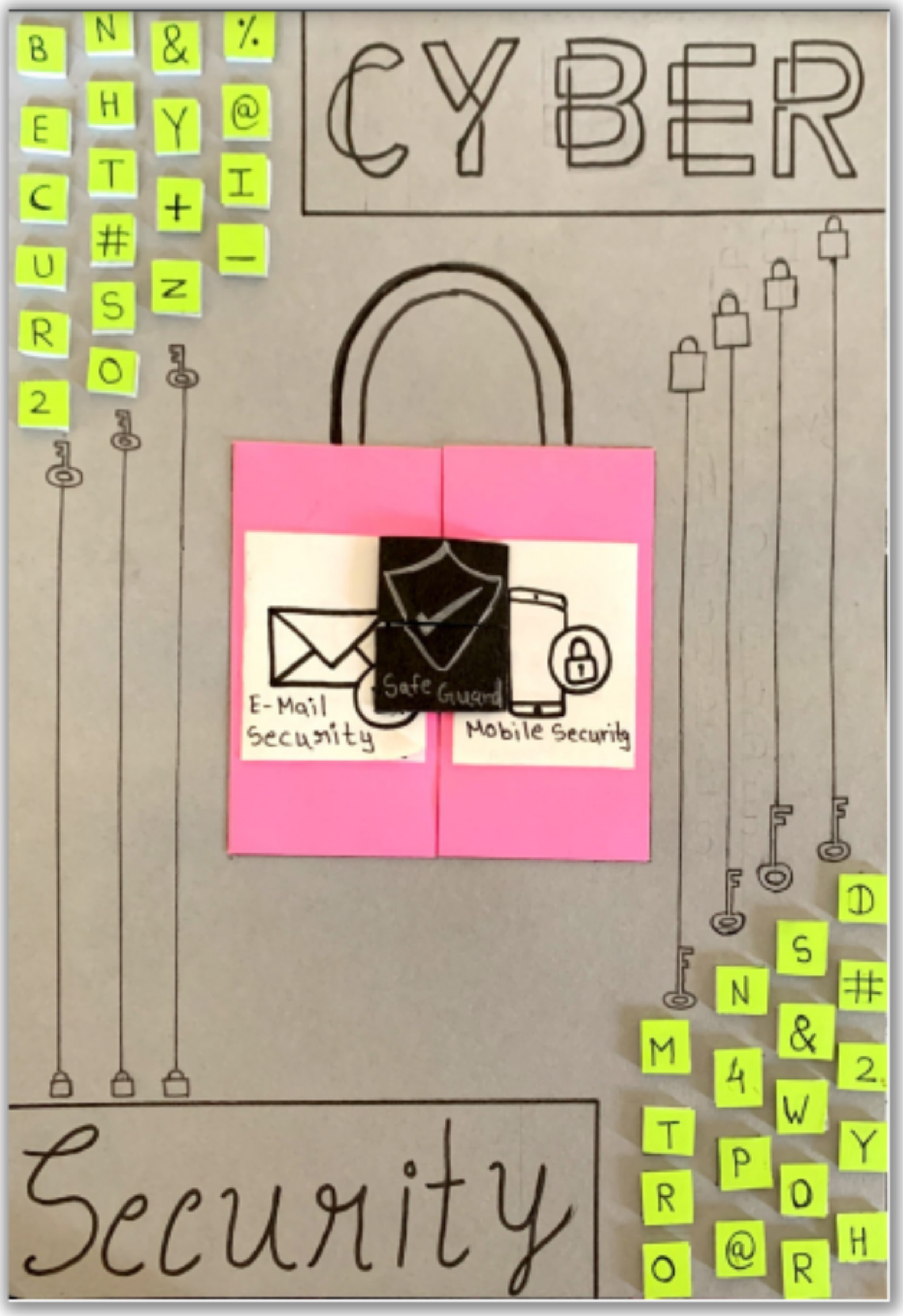
***Mr. Jeel Ghadiya** is a student of Grade IX at Radhika EduCare School, Jamnagar. He has prepared this poster for awareness of Cyber Security.*

CREATIVES


Digital Payment Security Tips
And Preventing Payment Frauds
I am Cyber SAFE
Identity Verification
Avoid Public Computers / Wifi networks
Buy only from Reliable websites
https://
https://
Beware of fraudulent Apps
6:54
Bank
Bank alert/ notification
Don't Share Password
Avoid Saving card details
VISA 424
Use a Private window for transactions

__Mr. Kevin Gada__ is a student of Grade-IX at Radhika EduCare School, Jamnagar. He has prepared this poster for Do's and Don'ts for Cyber Security Threats.

CREATIVES



Ms. Niti Bedia *is a student of Grade VIII at Radhika EduCare School, Jamnagar. She has prepared this poster for awareness on Cyber Security.*

Newsroom

Hour of Code 2022

An international event, the Hour of Code is celebrated on December 23, 2022 (Friday) at Shri. L. G. Haria School by Vague Foundation and Radhika EduVice. Other than Shri. L. G. Haria School, Radhika EduCare School, Jamnagar, and Radhika Classes, Jamnagar were also the participating institutes. The event was having two important aspects: (i) a celebration of the hour of code, and (ii) a project exhibition (coding projects by the students).

The event was inaugurated by Ms. Hetal Savla, Principal, CZMBCA College, Jamnagar in the august presence of Shri. Chandubhai Shah, Hon. Secretary, Oshwal Education Trust (OET); Dr. Bharteshbhai Shah, Trustee, OET, and Jain Educational Trust (JET); Ms. Jigna Pandya, Founder, Vague Foundation; SMC members of both schools, and various dignitaries in the field of education of Jamnagar.

The event was anchored by Mr. Raj Shah and Ms. Maulie Abraham followed by a presentation on Coding and a demonstration of the latest AI and ML-based tools.

More than 65 projects were exhibited by the students in the domains of Scratch, WordPress, and Canva from different institutes.

Mr. Dhaval Patt, Principal, LGHS, and Ms. Shivani Acharya, Principal, RES played pivotal roles in the organization of the event.

Shri. L. G. Haria School extended support for space, snacks, and organizational execution of the event.

Ms. Sheetal Bharadia (Event Coordinator) along with Ms. Vidhi Shah (CA) have seen the overall planning and execution.

Hour of Code was attended by 1000+ students, mentors, educators, and industrialists.

TRENDS - CYBER SECURITY

GOOD TWITTER HANDLES

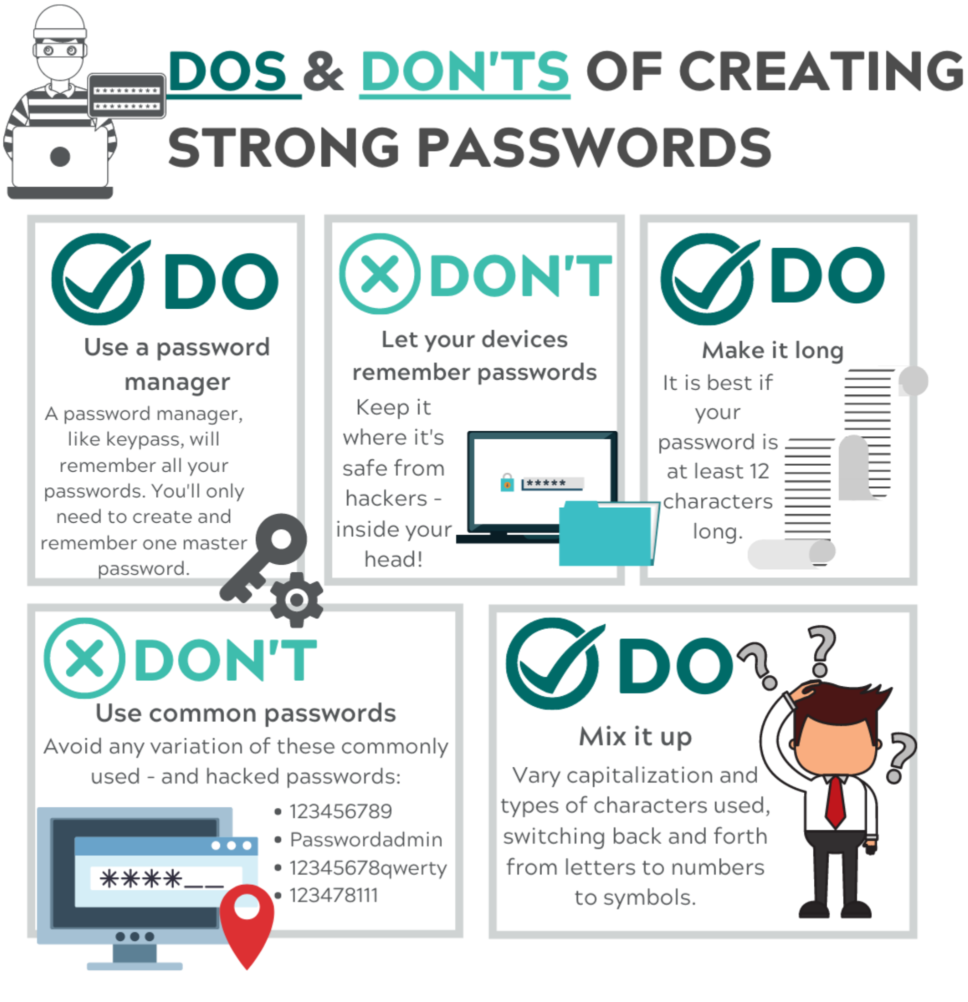
@THECYBERSECHUB

@STAYSAFEONLINE

GOOD BLOG TO READ

SCAN THESE QR-CODES TO GO

GOOD VIDEO TO SEE



DOS & DON'TS OF CREATING STRONG PASSWORDS

DO

Use a password manager

A password manager, like keypass, will remember all your passwords. You'll only need to create and remember one master password.

DON'T

Let your devices remember passwords

Keep it where it's safe from hackers - inside your head!

DO

Make it long

It is best if your password is at least 12 characters long.

DON'T

Use common passwords

Avoid any variation of these commonly used - and hacked passwords:

- 123456789
- Passwordadmin
- 12345678qwerty
- 123478111

DO

Mix it up

Vary capitalization and types of characters used, switching back and forth from letters to numbers to symbols.

GREY MATTER

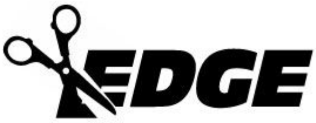
SUDOKU

		7	3		8	1		
	4		9		2		8	
		9		5		7		
9	5						1	6
3	8						2	7
		1		4		2		
	7		2		6		5	
		5	1		7	9		

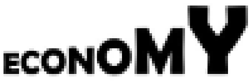
Rules: (i) Each row and column must contain the numbers from 1 to 9, without repetitions. (ii)The digits can only occur once per block

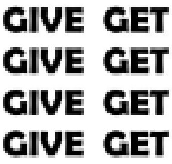
REBUS PUZZLE

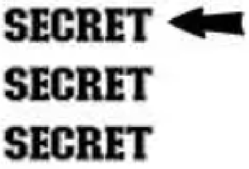
A rebus is a puzzle device that combines the use of illustrated pictures with individual letters to depict words or phrases. Rebus Writing can be a really helpful tool to incorporate into lessons at school, particularly those teaching Phonics. Because the Rebus principle focuses on pictographs representing single words, sounds and syllables, it can help children get to grips with specific phonemes they need to know and lateral thinking among students. Example:

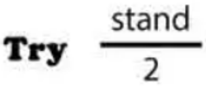


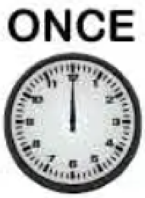
Cutting Edge











INVITATION & ANNOUNCEMENT

Theme based articles / essays are invited from the students and faculty members for the Upcoming Issue of **"Code-IT"**. The theme of the next issue is **Chatbot**. Selected articles will be published in this newsletter and an e-certificate will be given to the author(s). Authors can submit their article with photographs to **vaguefoundation@gmail.com** on or before **28/02/2023**.

Important Instructions:

- The article must be of 300 to 500 words.
- The article must be original (if taken from other website/material, please mention the source.)

Publisher

Vague Foundation
www.vaguefoundation.com
/vaguefoundation