SAFE & SECURE

PROTECTING YOURSELF IN THE DIGITAL WORLD

IN THIS PRESENTATION WE WILL COVER THE FOLLOWING TOPICS:

- Different types of cyber threats and real-world examples
- Tips and best practices for preventing cyber attacks
- Ways to protect yourself from cyber threats

THREATS: MALWARE

Malware is a broad category of malicious software that is designed to harm a computer or steal information.

Examples of malware include

Viruses	Trojan horses	Ransomware

Malware can be spread through email attachments, infected websites, and software downloads.

THREATS: PHISHING

Phishing scams are a type of social engineering that involves tricking individuals into giving away personal information, such as:

- Passwords
- credit card numbers
- Login credentials

These scams often use email, text messages, or social media to lure individuals into providing sensitive information.

Social engineering is a tactic used by cybercriminals to manipulate individuals into giving away personal information or access to their computer systems. This can include phishing scams, but also can include pretexting, and baiting.

THREATS: REAL-WORLD EXAMPLES

The WannaCry ransomware attack in 2017, which affected more than 200,000 computers in 150 countries.

The Equifax data breach in 2017, in which personal information of over 147 million people was exposed.

WANNACRY RANSOMEWARE ATTACK

- THE WANNACRY RANSOMWARE ATTACK WAS A CYBER ATTACK THAT OCCURRED IN MAY 2017 AND AFFECTED MORE THAN 200,000 COMPUTERS IN 150 COUNTRIES. THE ATTACK USED A TYPE OF MALWARE CALLED RANSOMWARE, WHICH ENCRYPTS A VICTIM'S FILES AND DEMANDS PAYMENT IN EXCHANGE FOR THE DECRYPTION KEY.

WANNACRY TARGET: MICROSOFT SYSTEMS

- THE WANNACRY RANSOMWARE SPECIFICALLY TARGETED A VULNERABILITY IN MICROSOFT WINDOWS OPERATING SYSTEMS, WHICH ALLOWED THE MALWARE TO SPREAD RAPIDLY THROUGH NETWORKS. THE ATTACK AFFECTED A WIDE RANGE OF ORGANIZATIONS, INCLUDING HOSPITALS, GOVERNMENT AGENCIES, AND LARGE CORPORATIONS. MANY OF THE AFFECTED ORGANIZATIONS WERE FORCED TO SHUT DOWN THEIR SYSTEMS AND SOME HAD TO PAY A RANSOM TO REGAIN ACCESS TO THEIR FILES.

WANNACRY: A REMINDER TO KEEP SOFTWARE UP TO DATE

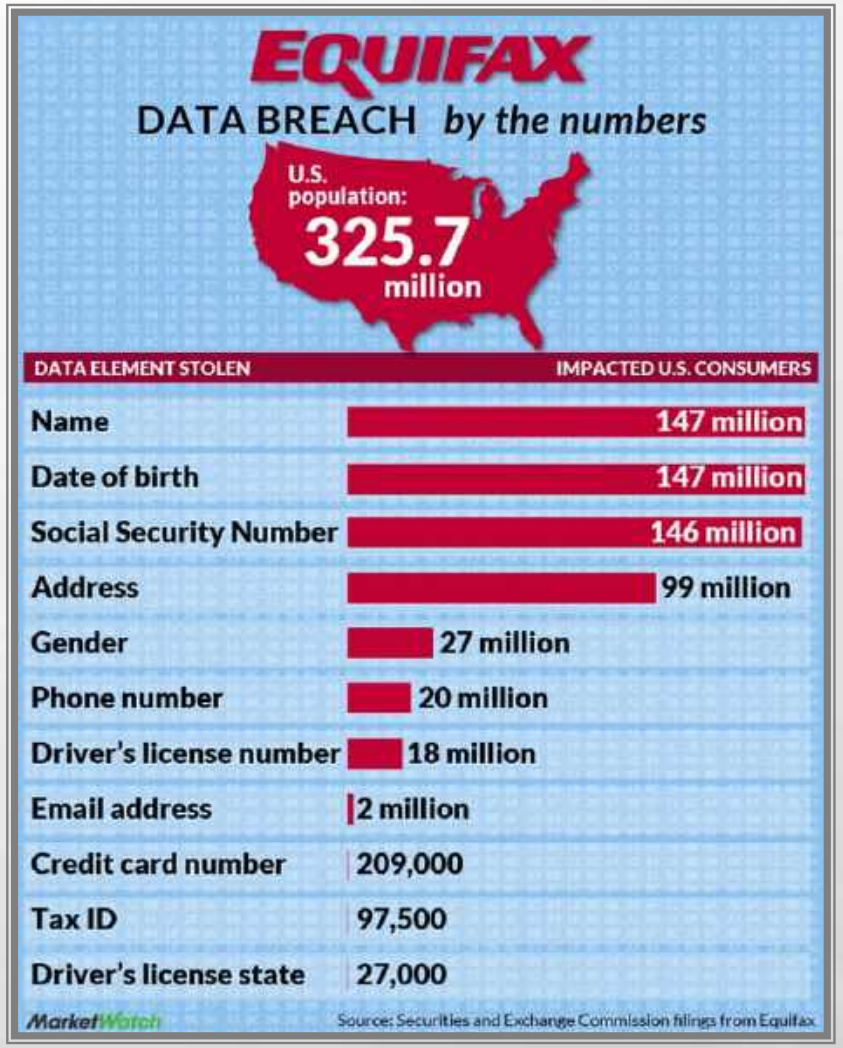
- THE ATTACK WAS PARTICULARLY NOTABLE FOR THE SPEED AT WHICH IT SPREAD, AS WELL AS THE LARGE NUMBER OF ORGANIZATIONS AND INDIVIDUALS AFFECTED. IT ALSO HIGHLIGHTED THE IMPORTANCE OF KEEPING SOFTWARE UP-TO-DATE AND PATCHING VULNERABILITIES IN A TIMELY MANNER.

WANNACRY HEARD AROUND THE WORLD

THE ATTACK PROMPTED A GLOBAL RESPONSE, WITH GOVERNMENTS, ORGANIZATIONS, AND INDIVIDUALS TAKING STEPS TO PROTECT THEMSELVES FROM FUTURE RANSOMWARE ATTACKS. IT ALSO HIGHLIGHTED THE IMPORTANCE OF HAVING A ROBUST CYBER SECURITY STRATEGY IN PLACE, INCLUDING REGULAR BACKUPS, SOFTWARE UPDATES, AND EMPLOYEE TRAINING.

EQUIFAX: DATA BREACH

- THE EQUIFAX DATA BREACH WAS A CYBER ATTACK THAT OCCURRED IN 2017, IN WHICH PERSONAL INFORMATION OF OVER 147 MILLION PEOPLE WAS EXPOSED. THE BREACH AFFECTED EQUIFAX, ONE OF THE THREE LARGEST CONSUMER CREDIT REPORTING AGENCIES IN THE UNITED STATES, AND RESULTED IN THE COMPROMISE OF SENSITIVE INFORMATION, SUCH AS NAMES, ADDRESSES, SOCIAL SECURITY NUMBERS, BIRTH DATES, AND DRIVER'S LICENSE NUMBERS. ADDITIONALLY, CREDIT CARD NUMBERS FOR AROUND 209,000 CONSUMERS, AND CERTAIN DISPUTE DOCUMENTS WITH PERSONAL IDENTIFYING INFORMATION FOR APPROXIMATELY 182,000 CONSUMERS WERE ACCESSED.



EQUIFAX: PROOF THAT BIG ORGANIZATIONS ARE NOT SAFE EITHER

- THE EQUIFAX DATA BREACH SERVES AS A REMINDER OF THE IMPORTANCE OF HAVING ROBUST CYBERSECURITY MEASURES IN PLACE AND THE FACT THAT ORGANIZATIONS HAVE A RESPONSIBILITY TO PROTECT PERSONAL INFORMATION. IT ALSO HIGHLIGHTS THE IMPORTANCE OF BEING VIGILANT AND TAKING STEPS TO PROTECT PERSONAL INFORMATION, AS EVEN THE MOST WELL-ESTABLISHED ORGANIZATIONS CAN FALL VICTIM TO CYBER ATTACKS.

PREVENTION: 9 STEPS TO SAFE&SECURE

- TO PREVENT CYBER ATTACKS, IT'S IMPORTANT TO TAKE A PROACTIVE APPROACH AND IMPLEMENT BEST PRACTICES FOR PROTECTING YOURSELF. HERE ARE SOME TIPS FOR PREVENTING CYBER ATTACKS:

PREVENTION: 9 STEPS TO SAFE&SECURE

1

Use strong, unique passwords: Avoid using easily guessed passwords such as "password" or "1234" and use a combination of letters, numbers, and special characters. Avoid reusing the same password across multiple accounts.

2

Keep software and operating systems up-to-date: Cybercriminals often target vulnerabilities in older versions of software and operating systems. By keeping your software and operating systems up-to-date, you can protect yourself from these types of attacks.

PREVENTION: 9 STEPS TO SAFE&SECURE

3

Be cautious of unsolicited emails and messages: Cybercriminals often use phishing scams to trick individuals into giving away personal information. Be wary of unsolicited emails and messages, especially those that ask for personal information or login credentials.

4

Use anti-virus and anti-malware software: Anti-virus and anti-malware software can help protect your computer from malware and other malicious software. Make sure your software is up-to-date and run regular scans to detect any potential threats.

PREVENTION: 9 STEPS TO SAFE&SECURE

5

Use a VPN to protect your internet connection: VPNs encrypt your internet connection and protect your privacy, making it more difficult for cybercriminals to intercept your information.

6

Back up important files regularly: Backing up your files can help protect them in the event of a cyber attack. Consider using an external hard drive or a cloud-based backup service to store your backups.

PREVENTION: 9 STEPS TO SAFE&SECURE

7

Be careful when using public Wi-Fi networks: Public Wi-Fi networks can be vulnerable to cyber attacks. Avoid accessing sensitive information or entering login credentials while using public Wi-Fi networks.

8

Keep your personal information private: Be mindful of the information you share online and be careful of providing too much personal information.

9

Use two-factor authentication: Two-factor authentication adds an extra layer of security by requiring a second form of verification in addition to a password. This can help protect your accounts from being compromised by cybercriminals.

CONCLUSION

In summary, personal cybersecurity is an essential aspect of our digital lives. We have discussed the various types of cyber threats that individuals face, such as:		
malware,	phishing scams,	and social engineering,

we provided real-world examples to illustrate the seriousness of the issue.	
WannaCry ransomware attack	Equifax data breach

We also provided tips and best practices for preventing cyber attacks, such as:		
using strong passwords,	keeping software up-to-date,	and being cautious of unsolicited emails and messages.

Additionally, we discussed ways to protect oneself from cyber threats, such as:		
using anti-virus software,	firewalls,	and VPNs,

QUESTIONS...?

SOME THINGS I WOULD BE CURIOUS ABOUT:

WHAT TYPE OF JOB OPPORTUNITIES ARE IN CYBERSECURITY?

HOW IS CYBERSECURITY CHANGING FOR THE FUTURE?

THANK YOU FOR ATTENDING

PRESENTED & PRODUCED BY MRITALIAN.ONLINE & VILLAGEHELPDESK.COM