

CHOOSING A STRONG PASSWORD



Choosing a **hard-to-guess**,
but **easy-to-remember Pa\$\$w0rD** is important !



Use the following helpful tips to choose a strong password:

- Choose unique passwords with a combination of numbers, upper and lowercase alphabets and special characters
- Avoid using obvious personal information and dictionary words in your password
- Always use a long password (8 to 16 characters), consider using a phrase or abbreviations as your password
- Where feasible, consider using other technologies such as Multi Factor Authentication and Password-less Authentication.

.... Sample of a strong password:

"Twinkle, Twinkle Little Star How I Wonder What You Are?"

T T L S H I W W Y A

Now mix (upper/lower case), replace (alphabets with numbers) and sprinkle special characters as shown below

t T 1 * H ! W w u @

"tT1*H!Wwu@"
thus, forming a strong password



Treat your password like your toothbrush- choose a good one, don't share it with anyone, and change it periodically!



CYBER SECURITY TIPS



RANSOMWARE AWARENESS



Ransomware is a malicious software that locks and encrypts your device and threatens to deny access unless a ransom is paid

Ransomware Headlines

SECURITY Magazine
12.06.2020/FRIDAY #123456789
<https://www.securitymagazine.com>
Honda Pauses Production and Closes Offices due to Ransomware Attack

theguardian
24.07.2020/FRIDAY #123456789
<https://www.theguardian.com/>
Smartwatch maker Garmin hit by outages after ransomware attack: forced to shut down call centres, website and some other online services

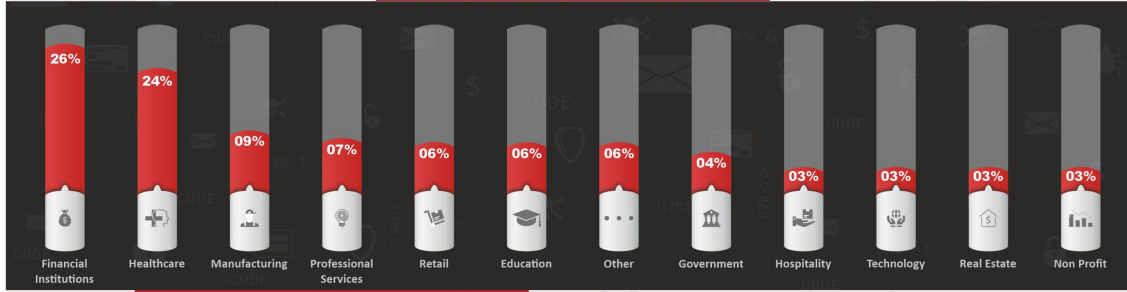
NEWS
21.07.2020/TUESDAY VOLUMES/EST.1987
Telecom Argentina S.A Hit by Major Ransomware Attack, Criminals Demand \$7.5M Worth of Monero

CYBERSECURITY NEWS
22.06.2020/MONDAY VOLUMES/EST.1987
Cognizant Says Maze Ransomware Attackers Hijacked Tax ID, Social Security, Passport Data

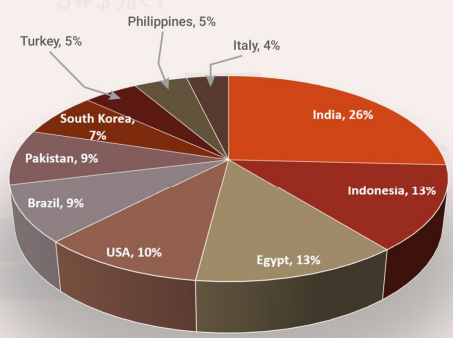
THE NEWS
02 JULY 2020/THURSDAY
Xerox becomes latest Maze ransomware victim

SECURITY BOULEVARD
30 JUNE 2020/TUESDAY
INTERPOL Says Ransomware Raids Against Hospitals Are on the Rise

Q1 2020 Ransomware Statistics



Ransomware attacks by countries



SecurityBoulevard: Ransomware statistics for 2020: Q1 report

HTTPS

67% of all malware was delivered via encrypted HTTPS connections
72% of encrypted malware was classified as zero day, so would have evaded signature-based antivirus protection

<https://www.helpnetsecurity.com/>

25%

25% increase in Ransomware compared to previous quarter.
"Beazley Breach Insight Report"

Following Do's and Don'ts can help protect you against Ransomware:

DO'S

- 🔒 Browse only trusted websites
- 🔒 Install mobile apps only from official app stores
- 🔒 Backup data as per your organization policies
- 🔒 Encrypt personal backups and keep it offline
- 🔒 Update OS & applications with latest patches
- 🔒 Update anti-virus and anti-malware software

DON'TS

- 🔒 Open suspicious email attachments
- 🔒 Click Links/banners in emails/websites
- 🔒 Install unauthorized software or unlicensed OS
- 🔒 Use untrusted USB devices
- 🔒 Use public or unsecured Wi-Fi connections.
- 🔒 Use public mobile charging points

In case you fall victim to ransomware:

- 🔒 Disconnect your system from the network
- 🔒 Report immediately to InfoSec team
- 🔒 For personal devices, rebuild your system from scratch
- 🔒 Avoid paying ransom as it encourages criminals





10

EASY WAYS TO PROTECT YOUR SMARTPHONE

-  Enable strong authentication (PIN, face recognition, finger print etc)
-  Only connect to known Wifi or use your Mobile data
-  Keep Bluetooth turned off, if not needed
-  Keep the OS and Apps updated
-  Set up remote locate/wipe
-  Restrict permissions to apps (location, camera, Bluetooth, etc.)
-  Use an up-to-date anti-virus/ anti-malware App
-  Install apps only from official App Stores
-  Do not use jailbroken/ rooted devices
-  Back-up your data periodically



Smartphones have become a way of life, be smart and protect your phone against cyber crime.