PKSIG

Cyber Security Awareness Session 22-08-2019

Ahmed Bakht Baloch
Deputy Director (Cyber Security)

Security Concerns

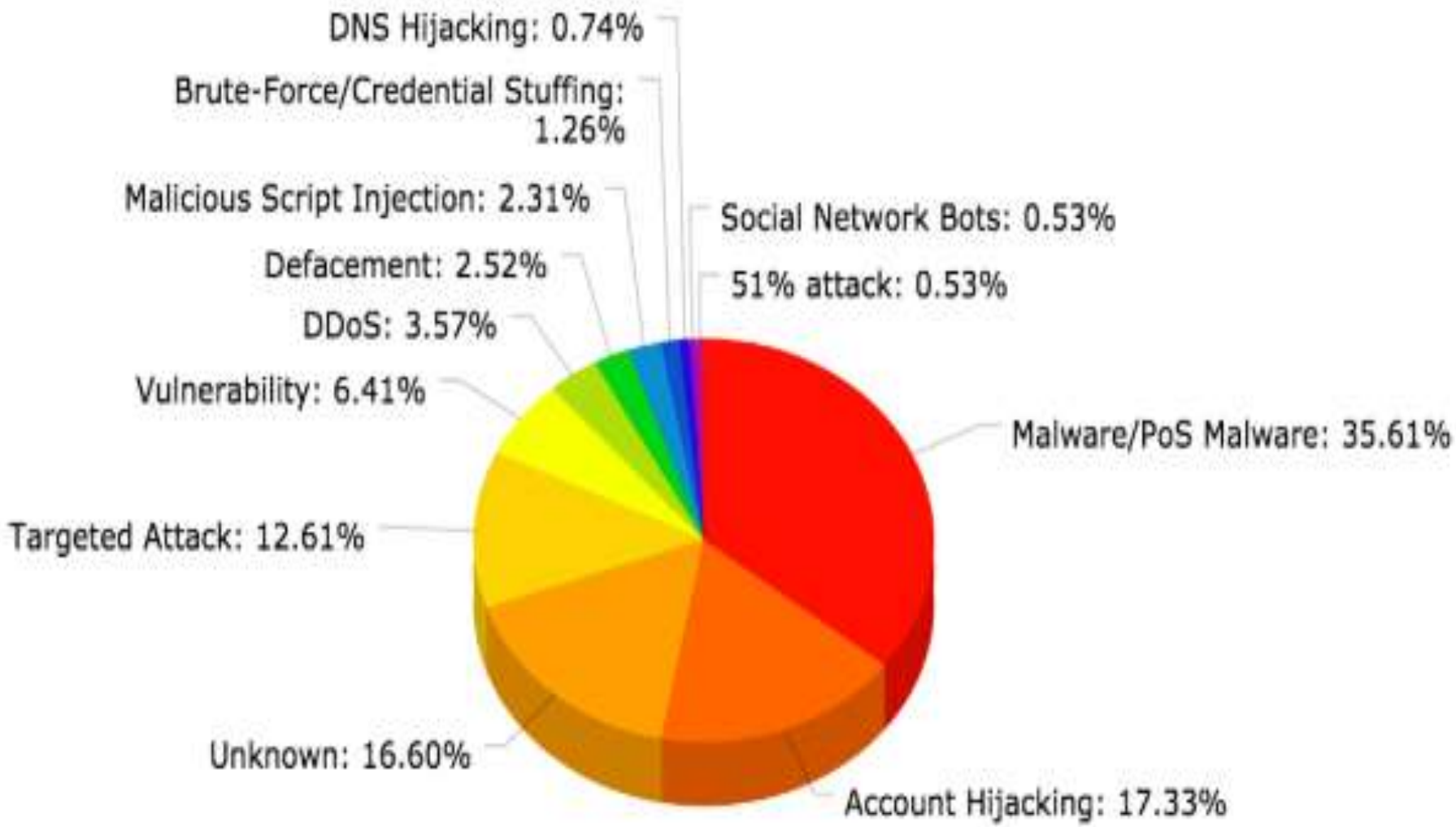
- Large Companies like Google / Apple
- Law Enforcement Agencies
- Hacking
- Misusage

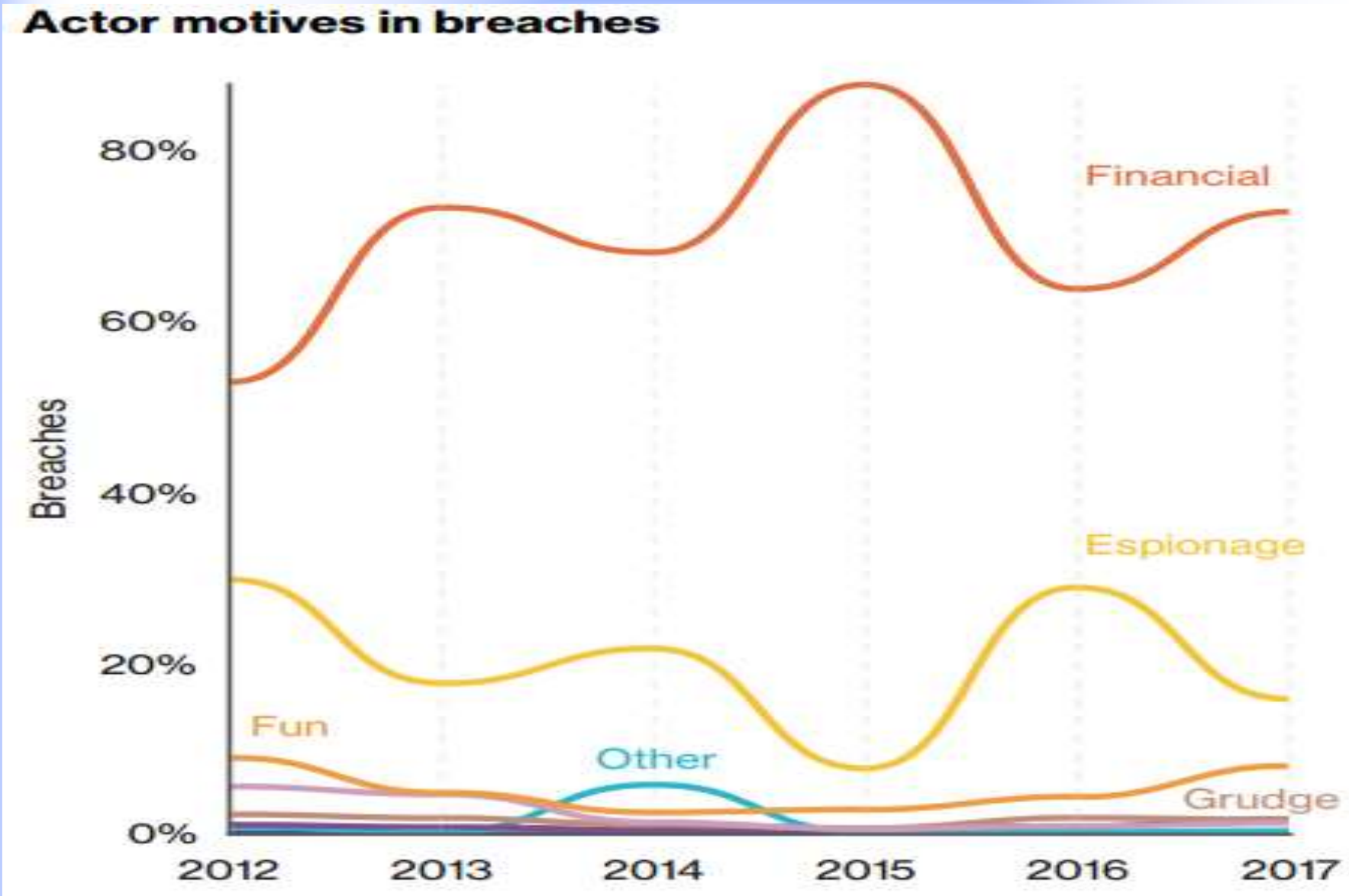
Responsibility

- Relevant Country / Region
  - Laws
  - Regulations
- Organization
  - Firewalls
  - Anti Virus
  - Spam Filters
- End Users
  - Careful usage

arts

Attack Distribution (Top 10 2018)

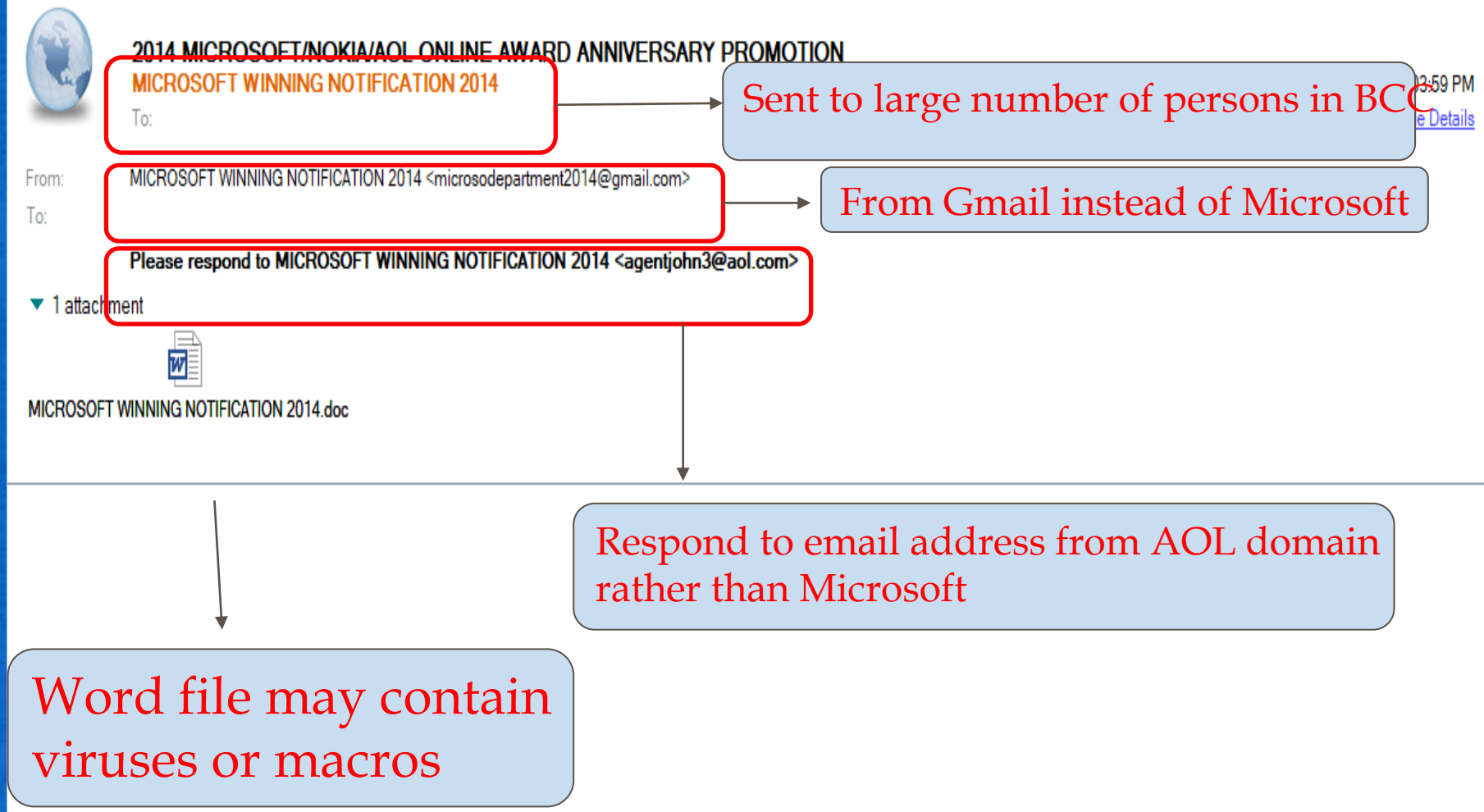




Source: Verizone Data Breach Research report 2018


PHISHING
The use of email 'lures' to try and entice unsuspecting victims to disclose private information
SPEARPHISHING
A highly targeted phishing attack targeting a specific group of individuals or organization
WHALING
A spear phishing attack focused on 'bigger fish' such as high ranking public or executive figures
SMISHING
Phishing SMS messages sent to smartphones
VISHING
Where an attacker phones the victim

Phishing Email Example



Threat: Password Security

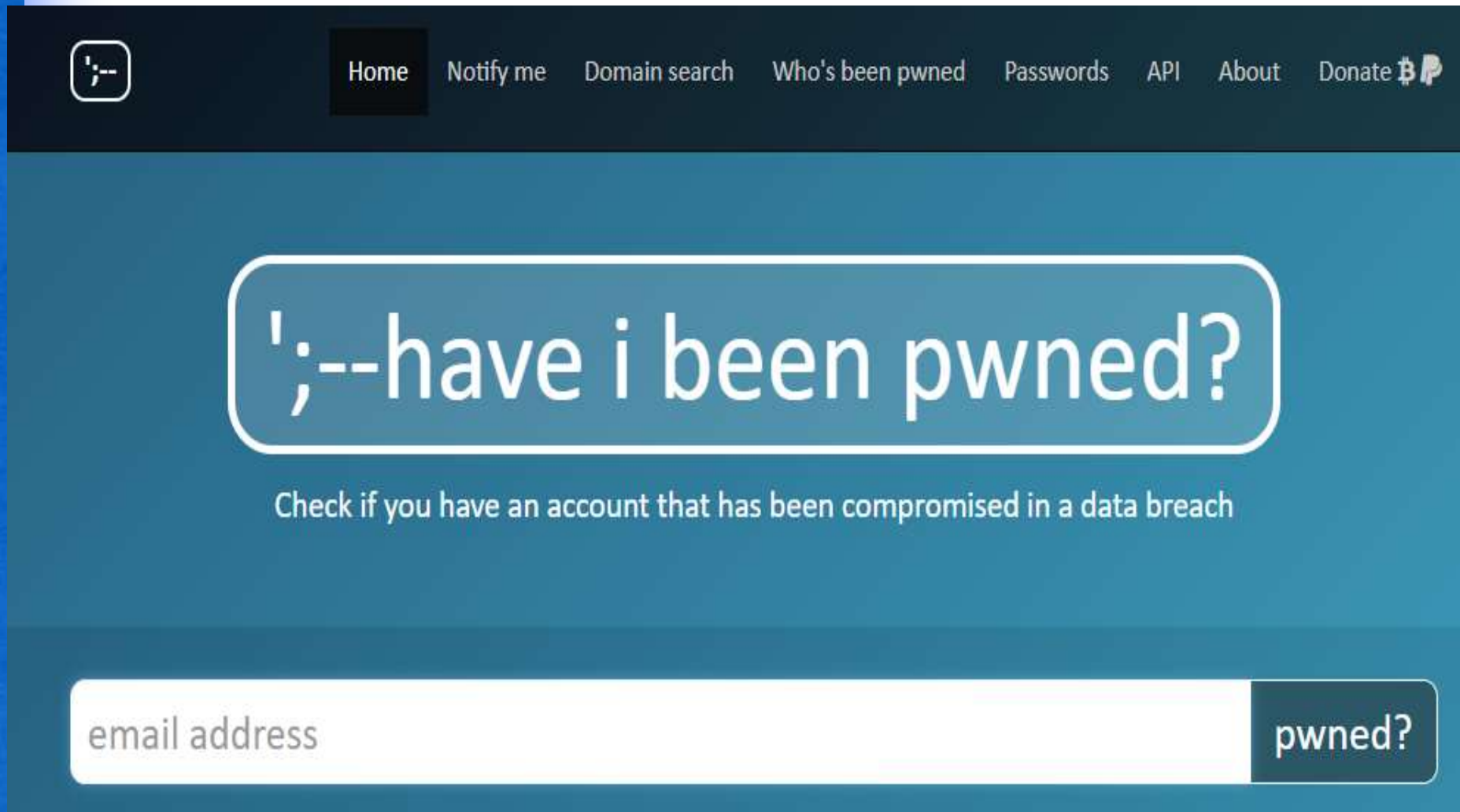
- Brute Force
- Guessing password
- Hacking
- Malware
- Phishing


Top 25 Worst Password of 2018
Determined By SplashData, Inc
1. 123456 (rank unchanged since 2017 list)
2. password (unchanged)
3. 12345678 (up 1)
4. qwerty (up 2)
5. 12345 (down 2)
6. 123456789 (new)
7. letmein (new)
8. 1234567 (unchanged)
9. football (down 4)
10. iloveyou (new)
11. admin (up 4)
12. welcome (unchanged)
13. monkey (new)
14. login (down 4)
15. abc123 (down 1)
16. starwars (new)
17. 123123 (new)
18. dragon (up 1)
19. passw0rd (down 1)
20. master (up 1)
21. hello (new)
22. freedom (new)
23. whatever (new)
24. qazwsx (new)
25. trustno1 (new)

Best Practices: Password Security

- Effective passwords are:
  - Long
  - Complex
  - Unique
  - Rotating
  - Do not save in the browsers

Email hacks

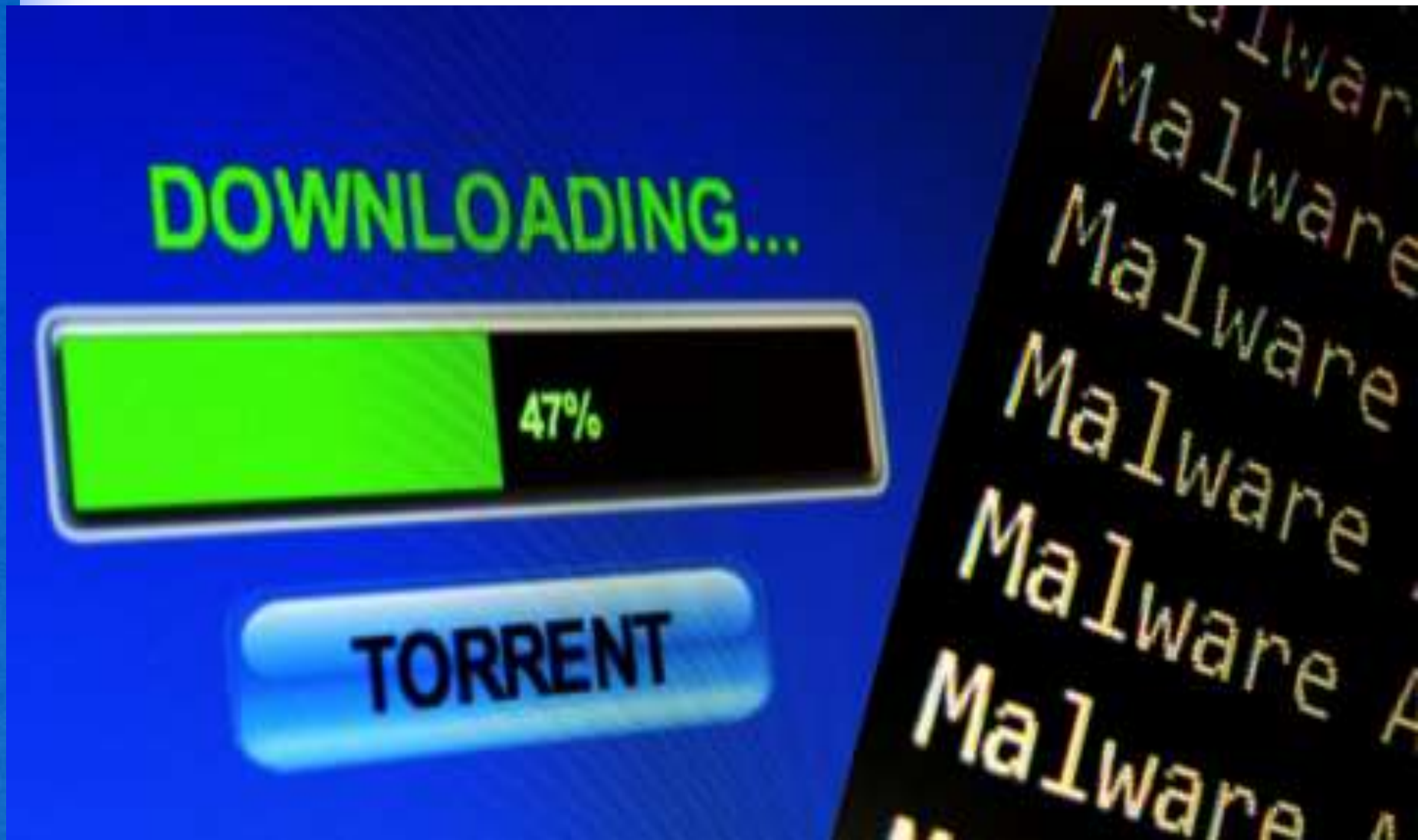

Home
Notify me
Domain search
Who's been pwned
Passwords
API
About
Donate
';--have i been pwned?
Check if you have an account that has been compromised in a data breach
email address
pwned?

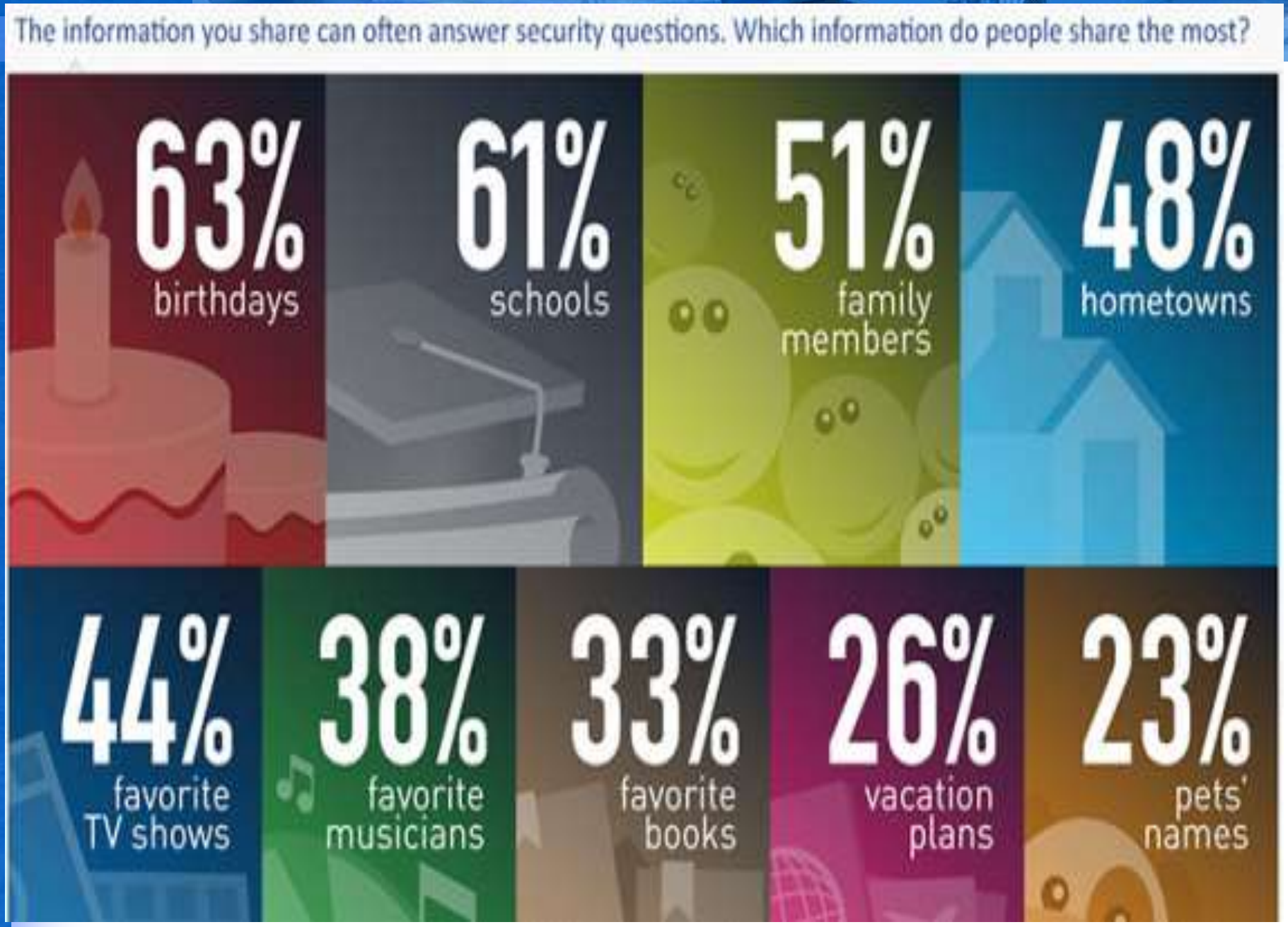
Best Practice: Browsing

- Protect your home Wi-Fi network with a password that only you and your family know
- Don’t store your passwords in your web browser
- Don’t click on pop-up ads or ads displayed on websites
- Limit the use of Cookies
- Try to limit your web browsing to sites that you’re familiar with or have prior knowledge of
- Websites can be “spoofed”- designed to look the same as a legitimate website but are instead used to deliver malware or steal sensitive information

Removable Media Threat

Torrents Security threat

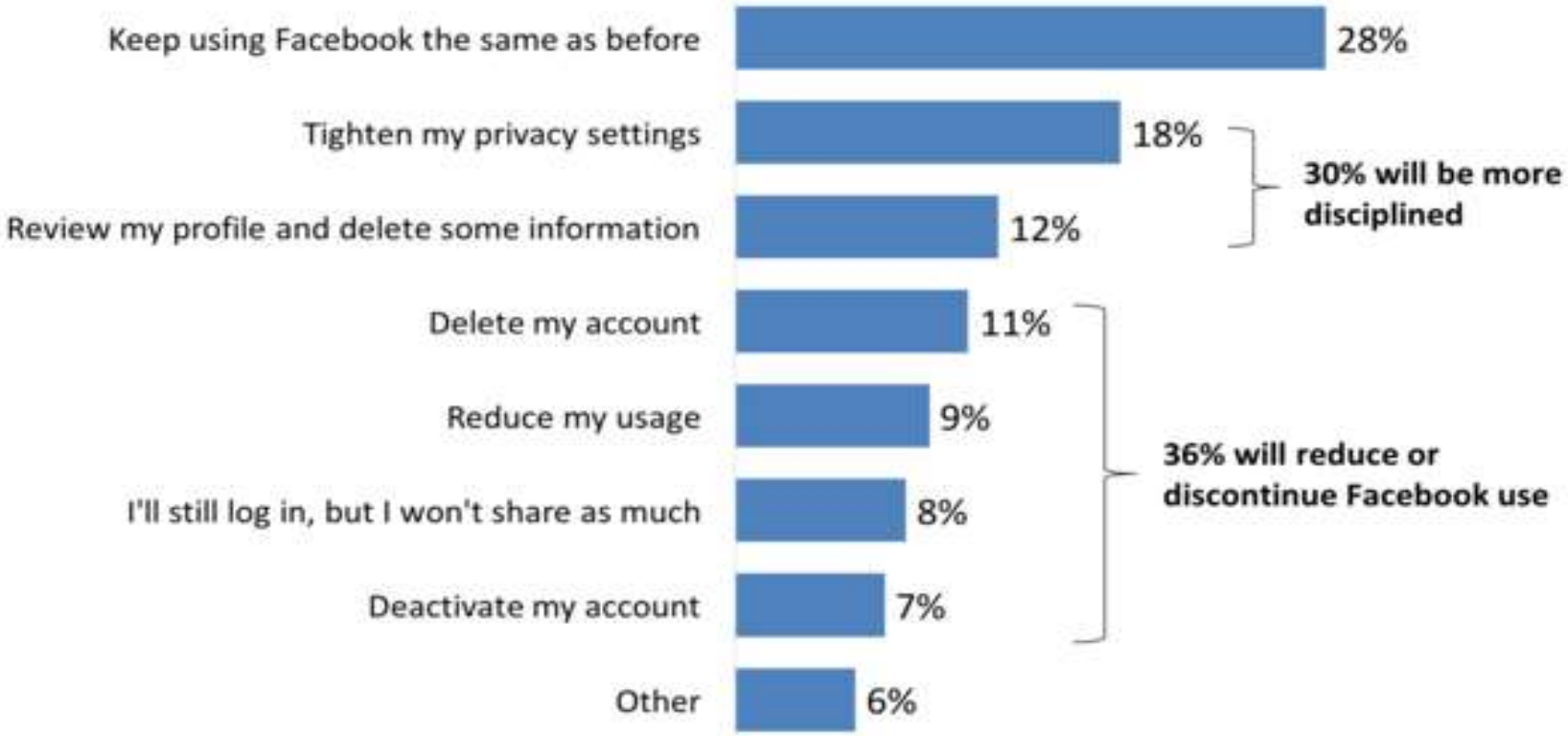




https://www.ezcomputersolutions.com/blog/security-risks-posed-social-media/

People whose Facebook information may have been improperly shared with Cambridge Analytica

Three In Four Facebook Users Say They'll Take Action Because Of Hack



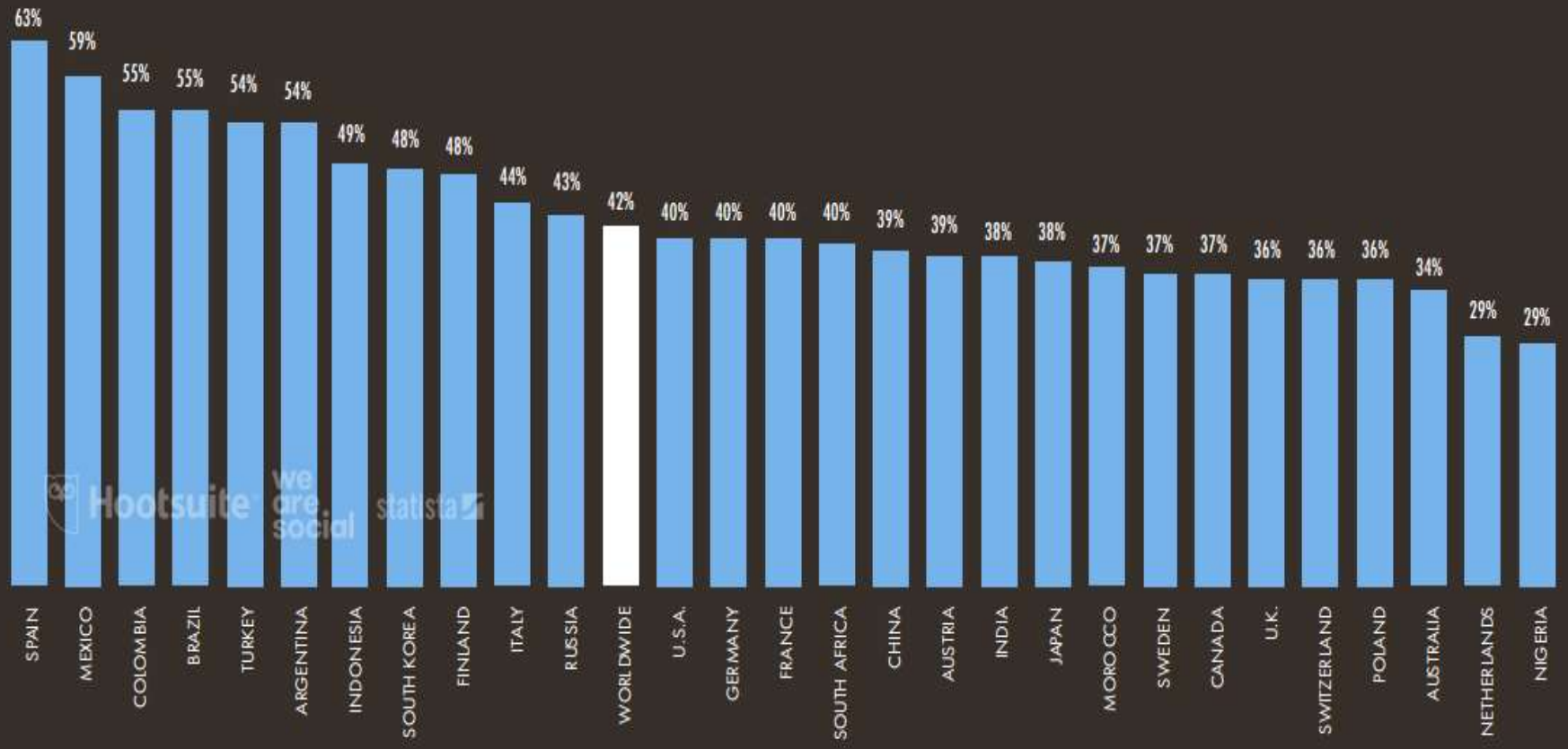
EXCLUSIVE DATA FROM BUSINESS INSIDER INTELLIGENCE

Q: Which action are you most likely to take as a result of the recent Facebook hack?
Source: Business Insider Intelligence Facebook Hack survey, n=2,676, 2018

JAN 2019

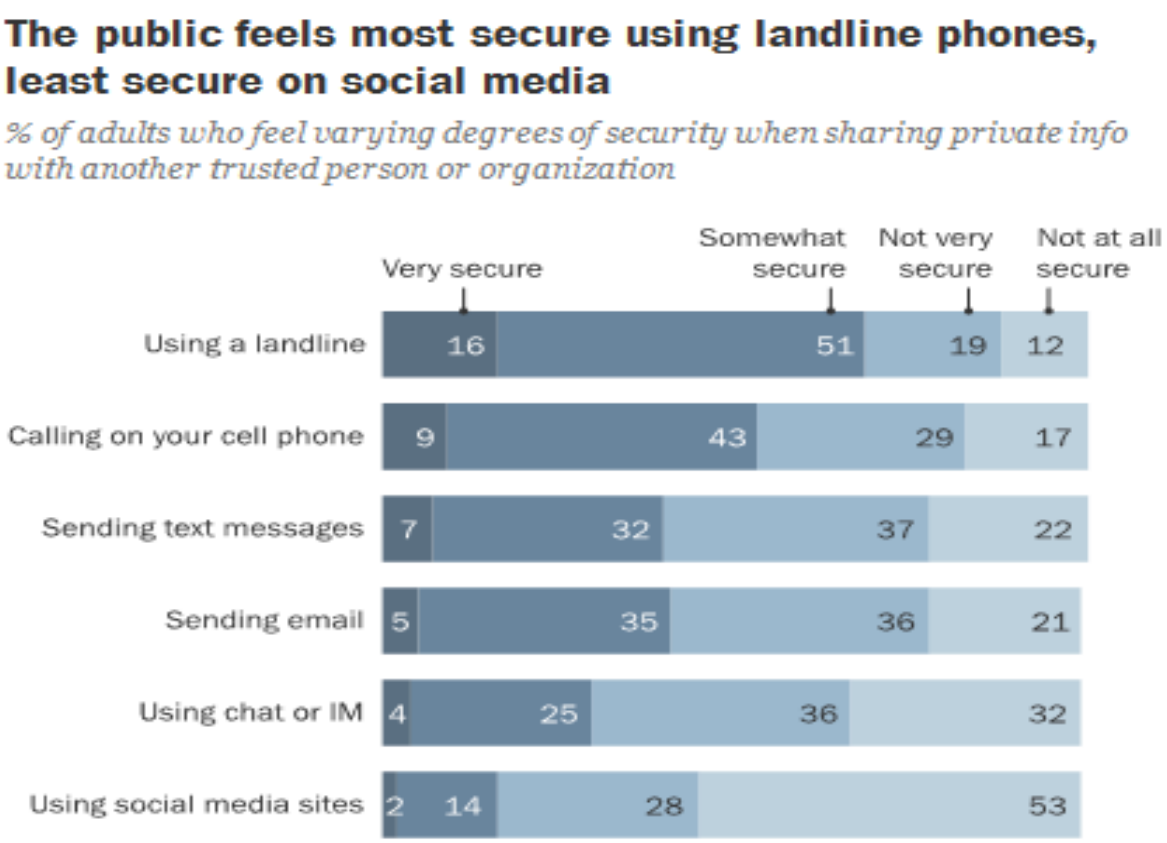
DATA PRIVACY CONCERNS

PERCENTAGE OF INTERNET USERS WHO BELIEVE THAT THEIR DATA IS BEING MISUSED ONLINE [SURVEY BASED]



SOURCE: STATISTA GLOBAL CONSUMER SURVEY 2018. *NOTE: FIGURE FOR 'WORLDWIDE' REPRESENTS AN AVERAGE OF FEATURED COUNTRIES THAT HAS BEEN WEIGHTED BY INTERNET PENETRATION IN EACH INDIVIDUAL COUNTRY.

The public feels most secure using landline phones, least secure on social media



Best Practices: Social Media

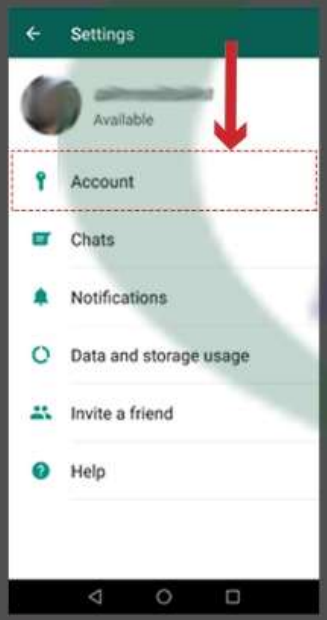
- Don’t “Over Share”
- Think before you share detailed information about yourself; could it be used to commit fraud?
- Simple Google Search can return information shared on social media sites
- Verify “Friend Requests”
- Do you really know this person?
- Does their profile seem legitimate?
- Understand and Use Privacy Features & Settings
- Consider making information like birthplace, birthday and employer “private”
- You can control who sees your social media profile, photos and posts!
- Select Strong Passwords

PROTECT YOUR WHATSAPP ACCOUNT AGAINST HIJACKING

Enable WHATSAPP Two-Step Verification to avoid hijacking

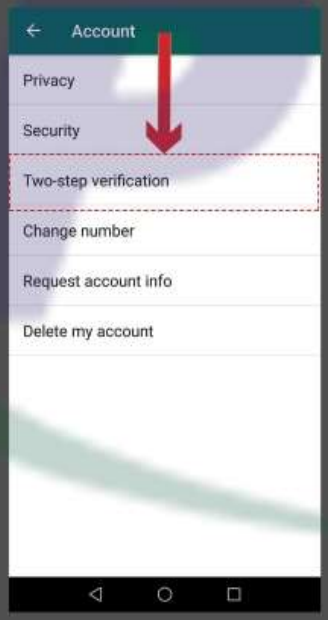
STEP - 01

1. Go to WhatsApp Settings and Click Account



STEP - 02

2. Click Two-Step Verification



STEP - 03

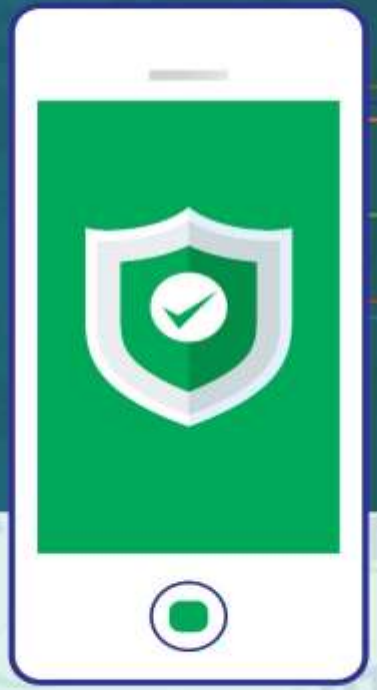
3. Click Enable

STEP - 04

4. Enter Same Six-Digit PIN twice
5. Enter Email address for future PIN recovery

A Public Awareness Message By Pakistan Telecommunication Authority

TIPS TO SECURE YOUR MOBILE HANDSET

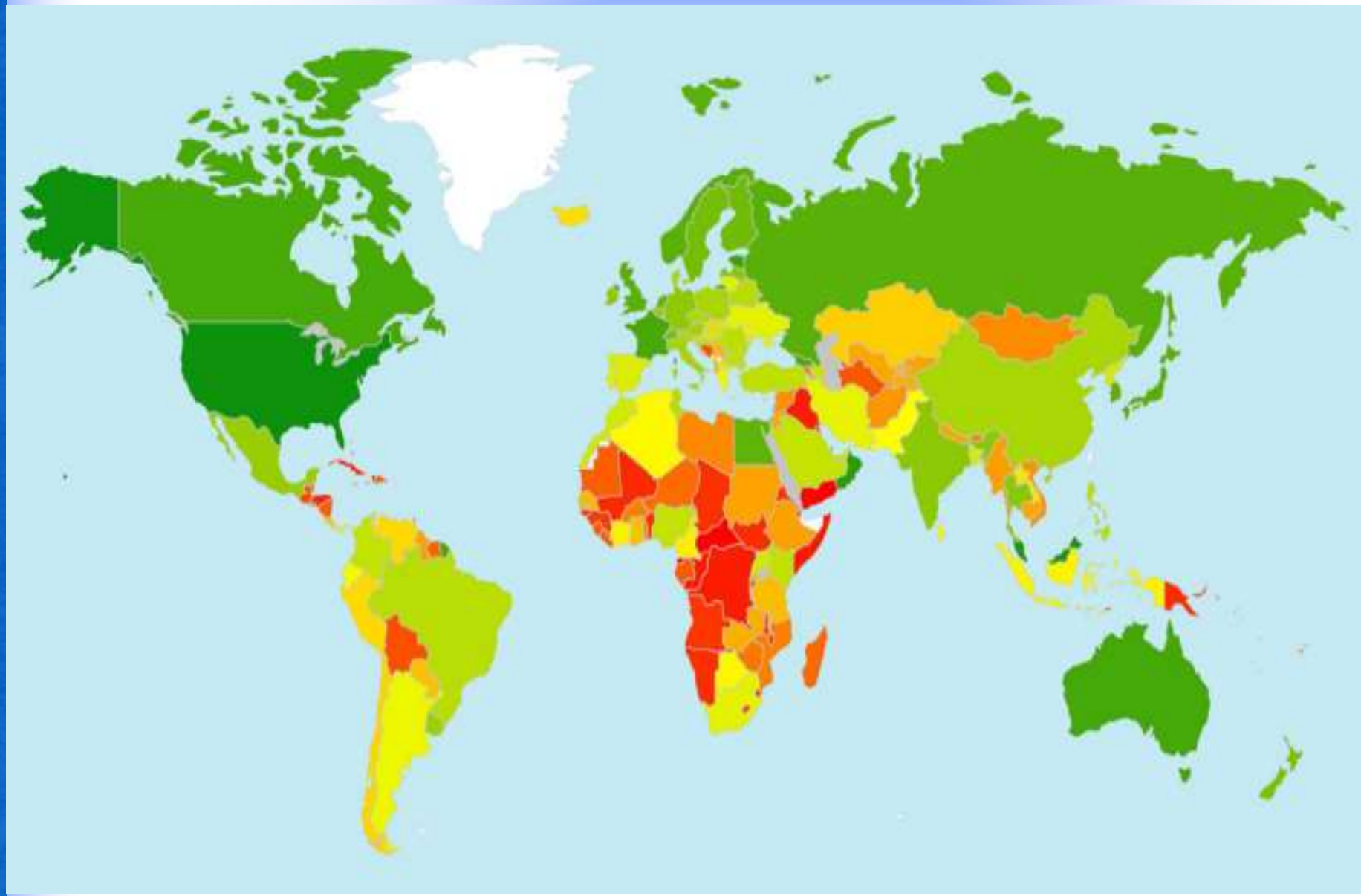


- Lock phone using a "PIN/Password" to avoid its misuse
- Install Apps only from "trusted Apps stores"
- Turn-off Bluetooth connection, after the usage
- Always encrypt your data on internal and external media
- Timely Installs updates / patches
- Always use a VPN on public WiFi / untrusted network

Only Buy PTA Approved Mobile Devices

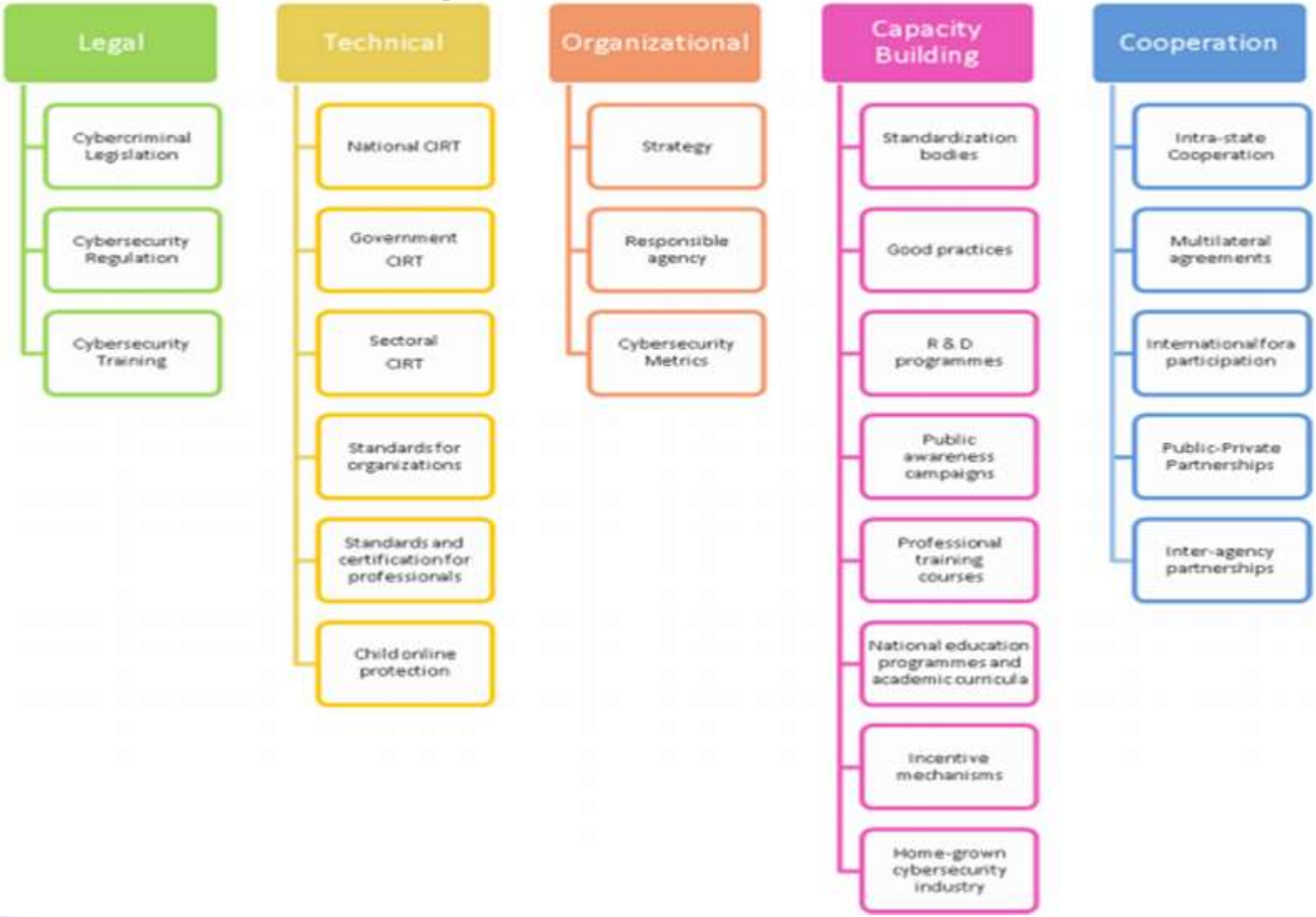
A Public Awareness Message By:
Pakistan Telecommunication Authority

PTA Headquarters, F-5/1, Islamabad
www.pta.gov.pk



Source: ITU Global Security Index 2017

Measuring Parameters



Source: ITU Global Security Index 2017

Table 6. Categories and Number of Security Devices Deployed

Category of Security Device	Number Deployed in the Network Infrastructure						Overall Response Count
	1–10	11–20	21–30	31–40	31–40	More than 50	
Firewalls (including next-generation firewalls)	39.4%	15.0%	11.9%	3.1%	1.6%	28.5%	99.5%
IDS/IPS (network-based)	51.3%	15.5%	6.7%	2.6%	1.6%	16.6%	94.3%
Malware detection	46.6%	6.2%	3.1%	1.6%	0.5%	32.1%	90.2%
Secure email gateways	71.0%	5.7%	4.7%	1.0%	0.0%	7.3%	89.6%
IDS/IPS (host-based)	30.6%	5.7%	3.1%	1.0%	0.5%	36.8%	77.7%
Web application firewalls (WAFs)	52.8%	7.8%	4.7%	1.6%	1.0%	8.8%	76.7%
Cloud access security brokers (CASB)	42.0%	6.2%	3.1%	1.0%	0.5%	4.1%	57.0%
Other	6.2%	1.0%	0.0%	0.0%	0.0%	1.6%	8.8%

Source: Network Security Infrastructure and Best Practices: A SANS Survey


Q&A