KEMENTERIAN SAINS, TEKNOLOGI DAN INOVASI
MINISTRY OF SCIENCE, TECHNOLOGY AND INNOVATION

An agency under MOSTI

CyberSAFE

MENDEPANI CABARAN KERAJAAN DIGITAL

Let's Make The Internet A Safer Place

www.cyberSAFE.my

Jazannul Azriq Aripin

Senior Executive, Outreach Dept., CyberSecurity Malaysia

Mr. Jazannul Azriq B. Aripin; Senior Executive of Outreach Department, CyberSecurity Malaysia. He has a degree in Computer Science from Universiti Malaysia Sabah. A Microsoft Certified System Engineer (MCSE) and ISMS Lead Auditor. Seven years with CyberSecurity Malaysia doing Facebook Security, Facebook Forensic, Information Security Audit (ISMS/ISO27001-2005) and Social Engineering

CyberSecurity MALAYSIA

An agency under MOSTI

CyberSAFE

Description

- CyberSAFE, short for Cyber Security Awareness For Everyone, is CyberSecurity Malaysia's initiative and Outreach Department tasked with educating and enhancing the awareness of the general public on the technological and social issues facing internet users, particularly on the risks they face online.

Let's Make The Internet A Safer Place

www.cyberSAFE.my

K	Y	P	O
Kids	Youth	Parents	Organisation

CyberSAFE

CyberSecurity MALAYSIA
An agency under MOSTI

SAFER INTERNET DAY 2015

10 FEBRUARY Let's create a better internet together

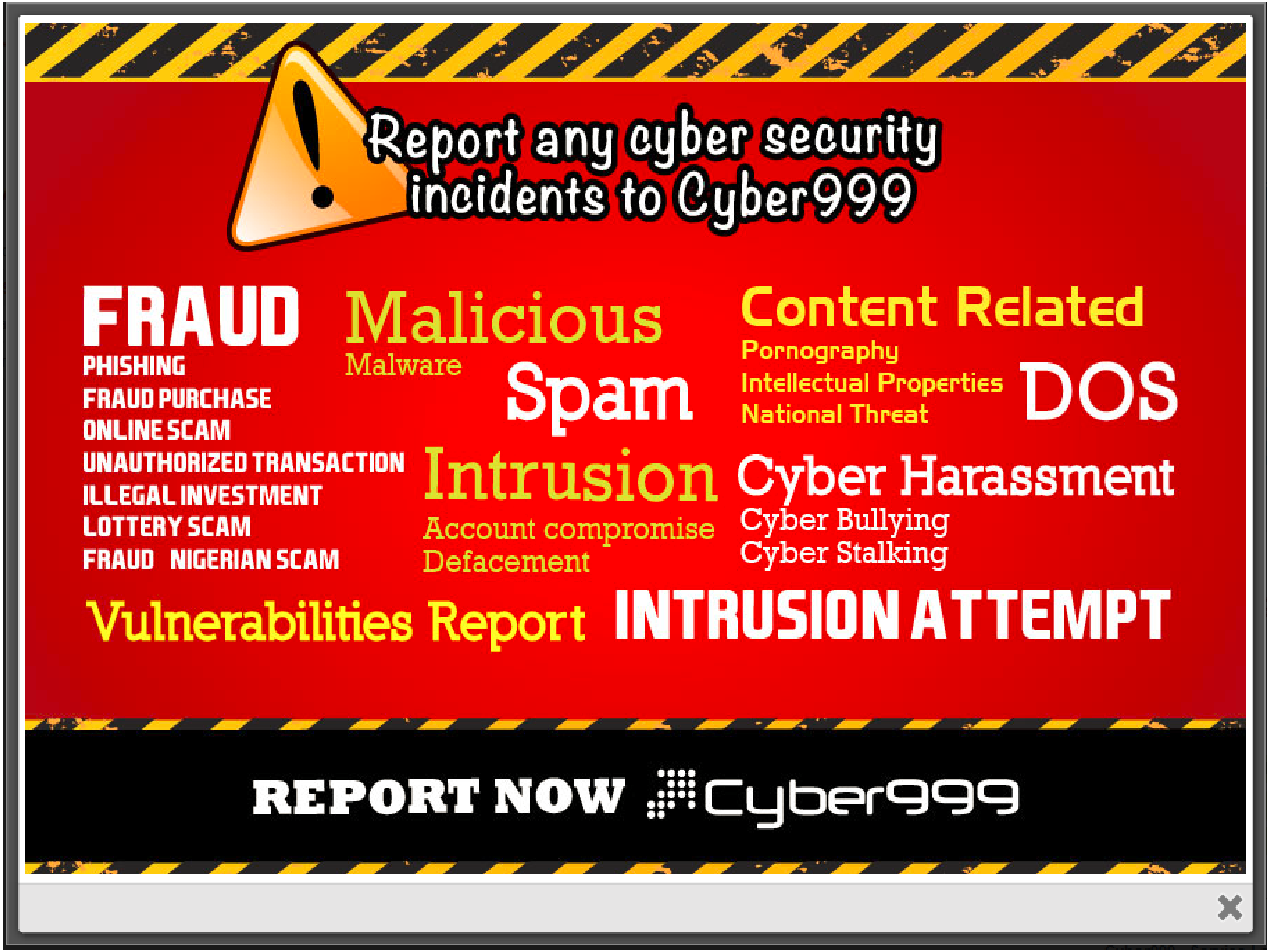
1. STRONG PASSWORDS
2. KNOW PRIVACY SETTINGS
3. CARE BEFORE SHARE

#LittleBigThing #SID2015

CYBERBULLYING: SAFEGUARD YOUR CHILDREN

Your guideline into the issue of cyberbullying amongst children

Download



Report any cyber security incidents to Cyber999

FRAUD

PHISHING
FRAUD PURCHASE
ONLINE SCAM
UNAUTHORIZED TRANSACTION
ILLEGAL INVESTMENT
LOTTERY SCAM
FRAUD NIGERIAN SCAM

Malicious

Malware

Spam

Content Related

Pornography
Intellectual Properties
National Threat

DOS

Intrusion

Account compromise
Defacement

Cyber Harassment

Cyber Bullying
Cyber Stalking

Vulnerabilities Report

INTRUSION ATTEMPT

REPORT NOW Cyber999

CyberSecurity MALAYSIA
An agency under MOSTI

MyCERT
Malaysia Computer Emergency Response Team

Cyber999

☎ 1300-88-2999 24x7
Emergency: +6019-266 5850

SMS Format: Cyber999 Report send to **15888**

cyber999 [at]cybersecurity.my

Fax +603-8945 3992

DOWNLOAD

Cyber999 Mobile Apps

Download on the App Store

GET IT ON Google play

MALAYSIA’S CYBER SECURITY INITIATIVES

National Cyber Security Policy

Thrust 1: Effective Governance

Thrust 2: Legislative & Regulatory Framework

Thrust 3: Cyber Security Technology Framework

Thrust 4: Culture of Security & Capacity Building

“Malaysia’s CNII shall be secure, resilient and self-reliant. Infused with a culture of security it will promote stability, social well being and wealth creation”

Critical National Information Infrastructure (CNII)

Thrust 5: R&D Towards Self Reliance

Thrust 6: Compliance & Enforcement

Thrust 7: Cyber Security Emergency Readiness

Thrust 8: International Cooperation

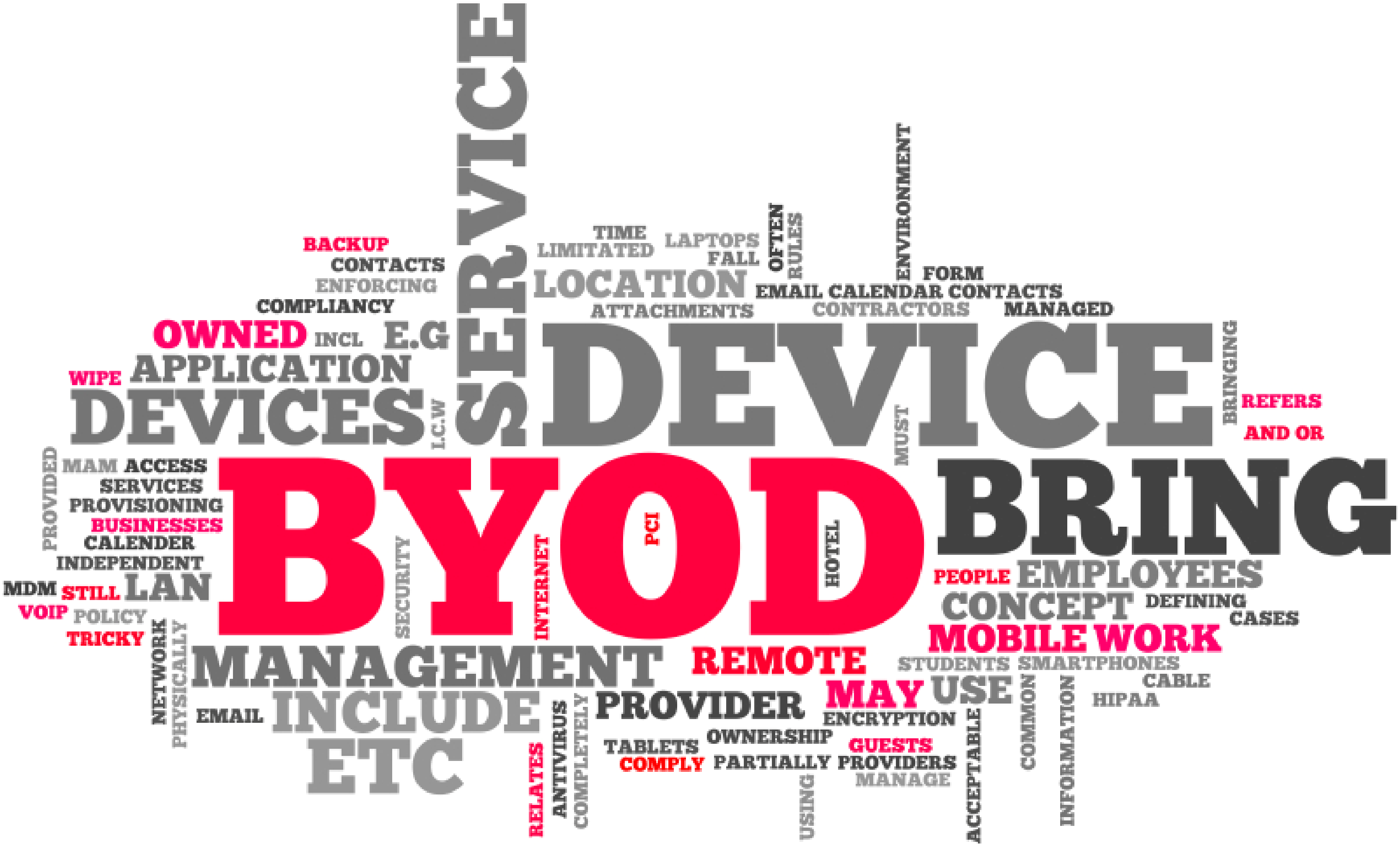
Security Scenarios I

Bad Guys' Perspective
Bad guys are constantly finding for the weakness of each components to ensure the success of malicious attack

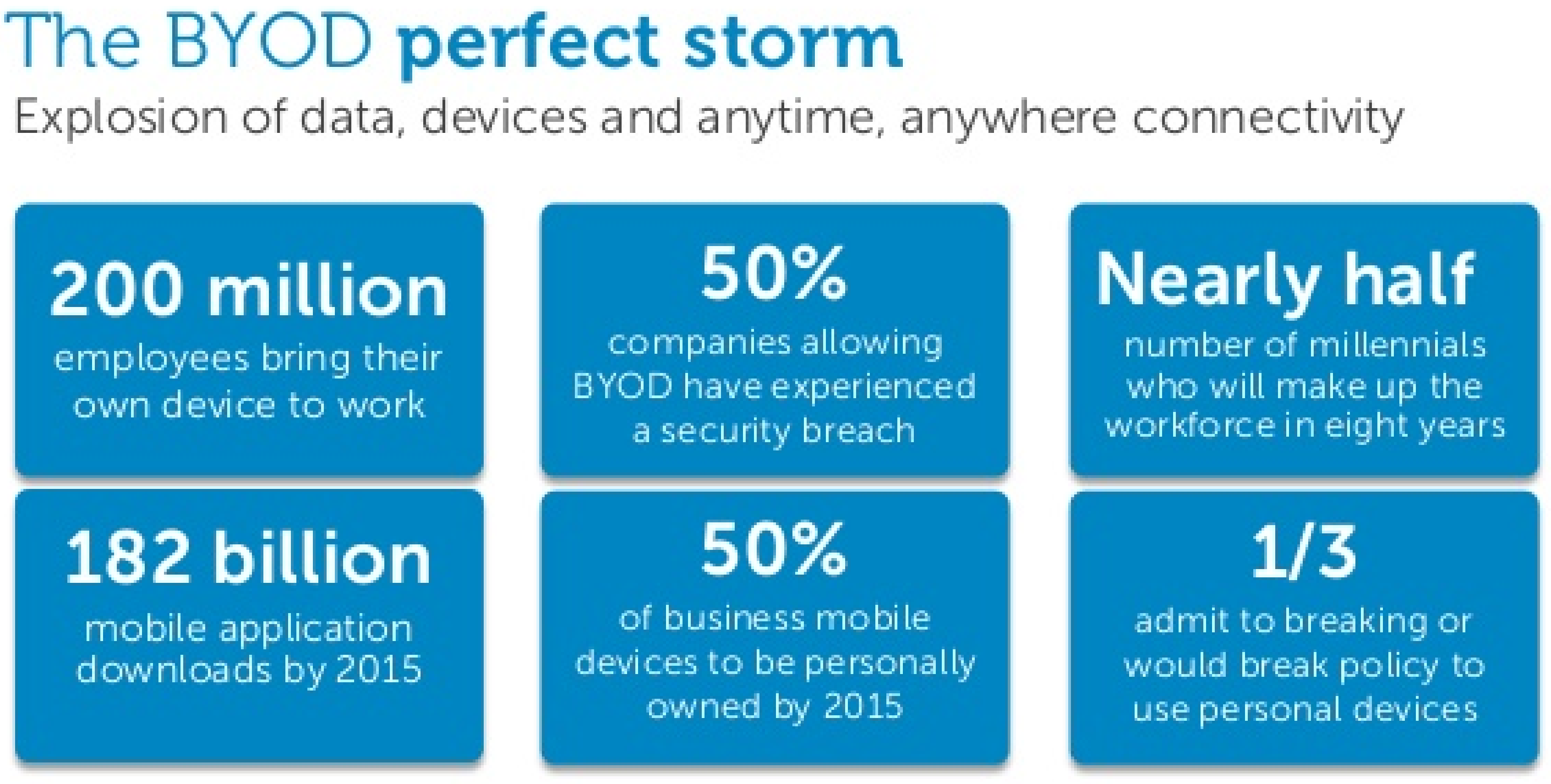
Users' Perspective
Most users are more focused on how to use computer to do their daily tasks but no so much about their security

"If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology" - Bruce Scheneir

#1 – BYOD


SERVICE
BACKUP
CONTACTS
ENFORCING
COMPLIANCY
TIME
LIMITATED
LAPTOPS
FALL
OFTEN
RULES
ENVIRONMENT
LOCATION
FORM
EMAIL CALENDAR CONTACTS
ATTACHMENTS
CONTRACTORS
MANAGED
OWNED
INCL
E.G
WIPE
APPLICATION
DEVICES
I.C.W
DEVICE
MUST
BRINGING
REFERS
AND OR
PROVIDED
MAM
ACCESS
SERVICES
PROVISIONING
BUSINESSES
CALENDER
INDEPENDENT
MDM
STILL
LAN
VOIP
POLICY
TRICKY
BYOD
SECURITY
INTERNET
PCI
HOTEL
BRING
PEOPLE
EMPLOYEES
CONCEPT
DEFINING
CASES
MOBILE WORK
NETWORK
PHYSICALLY
MANAGEMENT
REMOTE
STUDENTS
SMARTPHONES
CABLE
HIPAA
EMAIL
INCLUDE
PROVIDER
MAY
USE
COMMON
INFORMATION
ENCRYPTION
ETC
RELATES
ANTIVIRUS
COMPLETELY
TABLETS
COMPLY
OWNERSHIP
PARTIALLY
GUESTS
PROVIDERS
MANAGE
USING
ACCEPTABLE

#1 – BYOD



The BYOD **perfect storm**

Explosion of data, devices and anytime, anywhere connectivity

200 million
employees bring their own device to work

50%
companies allowing BYOD have experienced a security breach

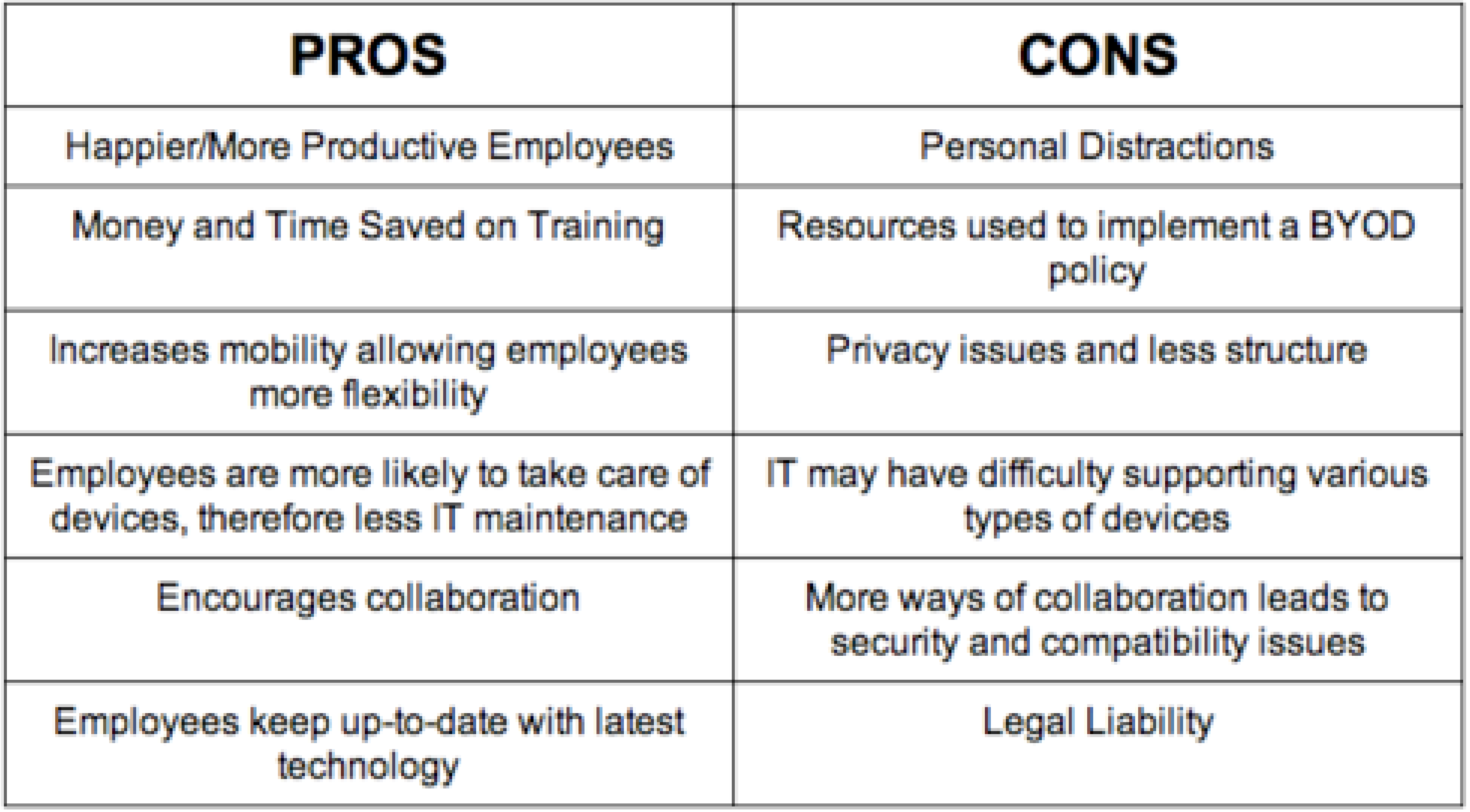
Nearly half
number of millennials who will make up the workforce in eight years

182 billion
mobile application downloads by 2015

50%
of business mobile devices to be personally owned by 2015

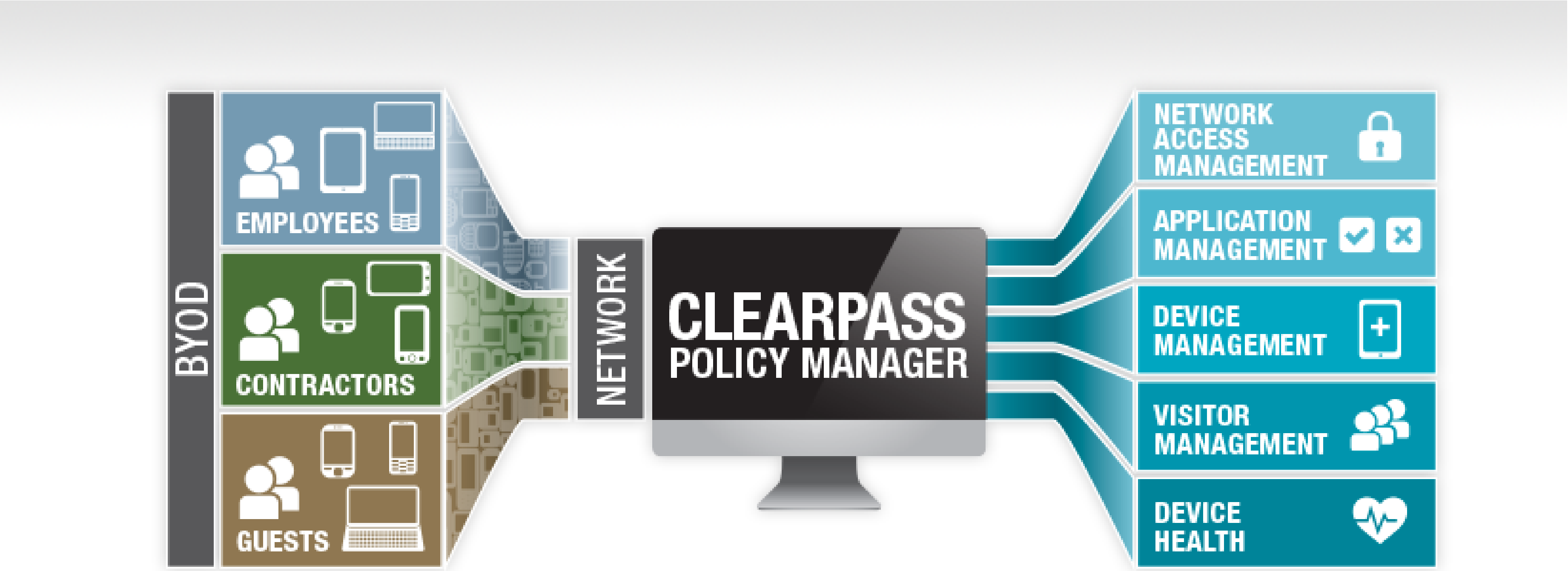
1/3
admit to breaking or would break policy to use personal devices

#1 – BYOD



PROS	CONS
Happier/More Productive Employees	Personal Distractions
Money and Time Saved on Training	Resources used to implement a BYOD policy
Increases mobility allowing employees more flexibility	Privacy issues and less structure
Employees are more likely to take care of devices, therefore less IT maintenance	IT may have difficulty supporting various types of devices
Encourages collaboration	More ways of collaboration leads to security and compatibility issues
Employees keep up-to-date with latest technology	Legal Liability

#1 – BYOD



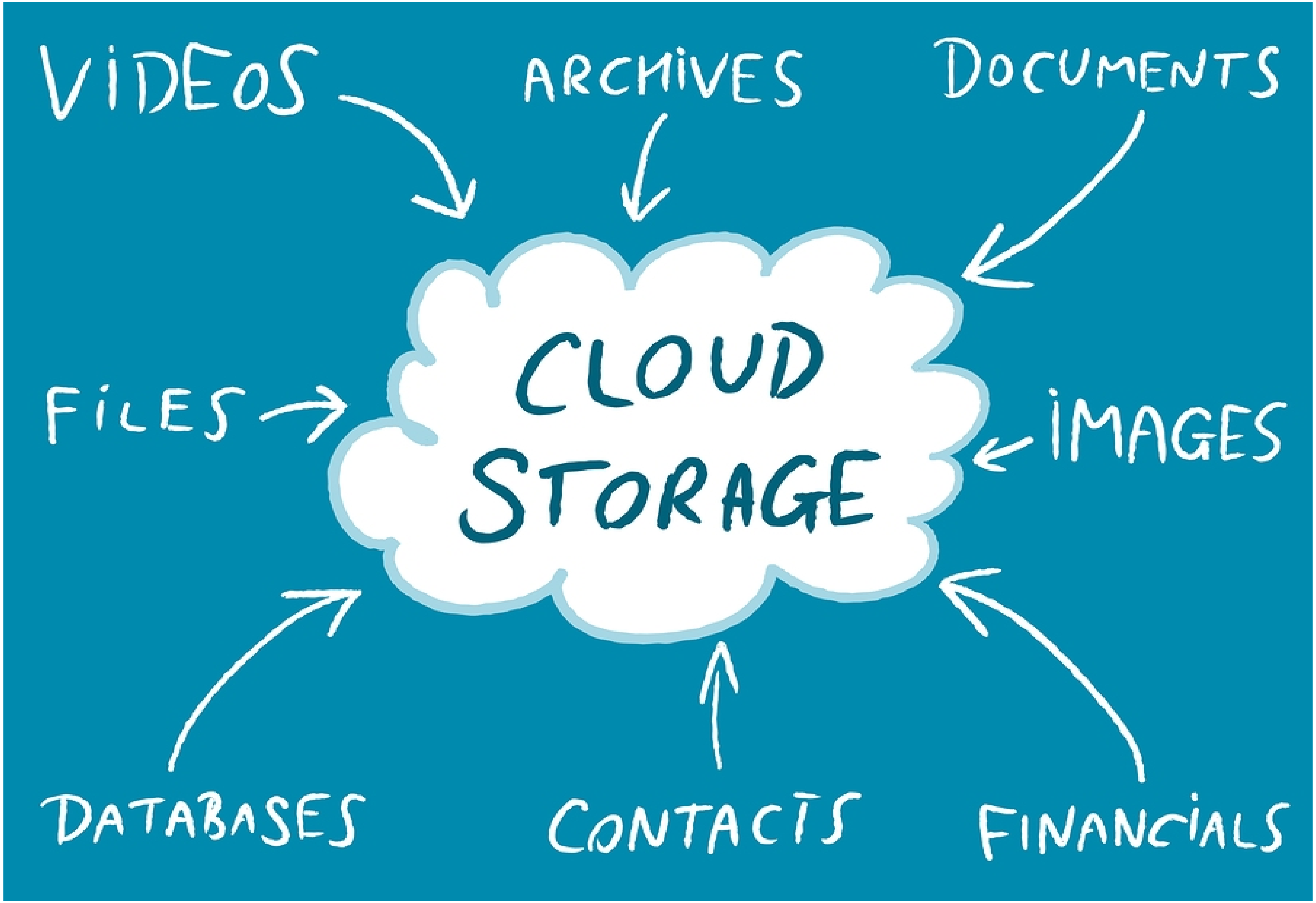
One place to manage all things BYOD

#2 – Cloud Services

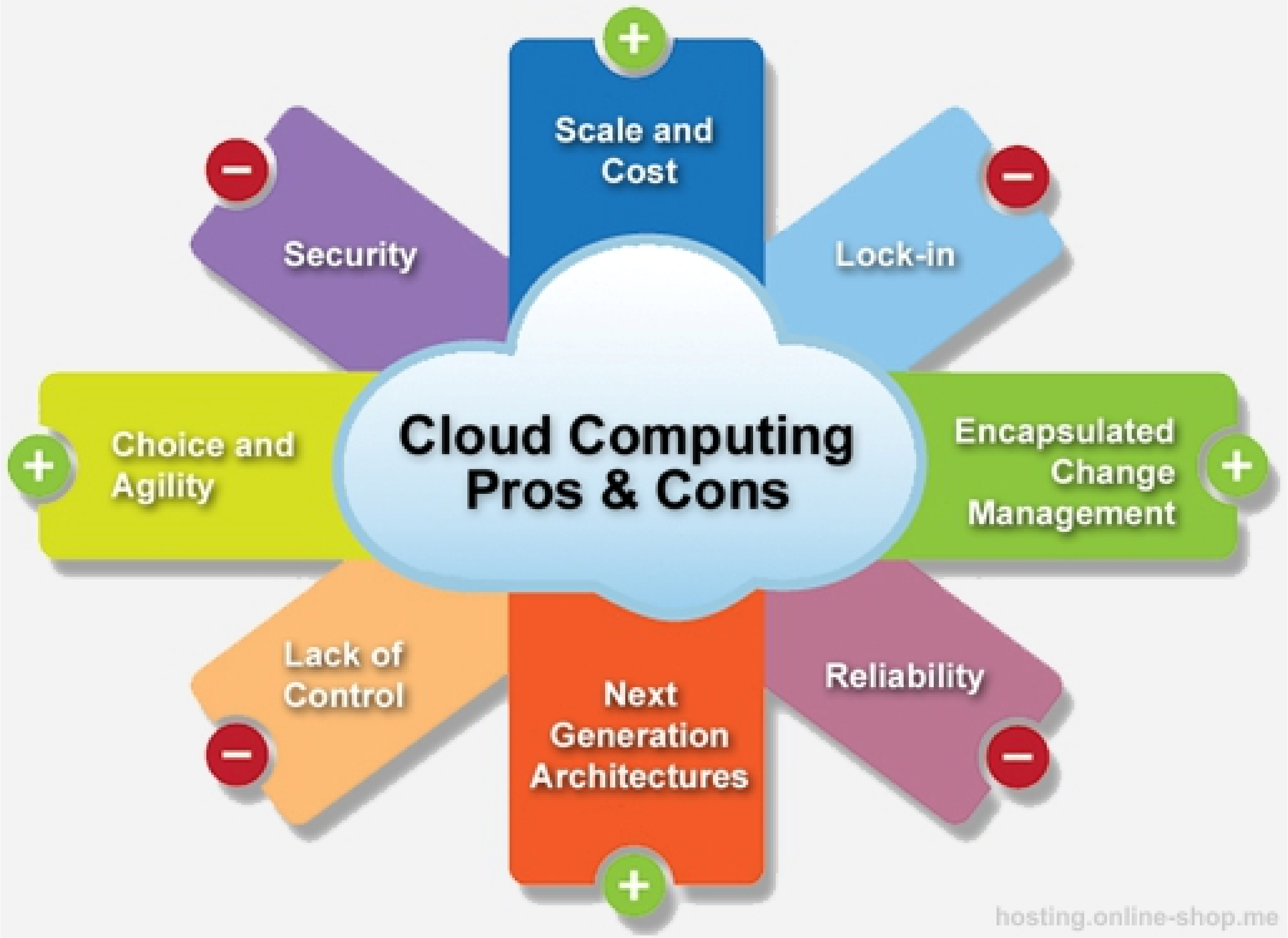
#2 – Cloud Services

zipcloud
box
justcloud.com
bitcasa
INFINITE STORAGE
Dropbox
OneDrive
IDrive®
Google Drive
MediaFire
iCloud

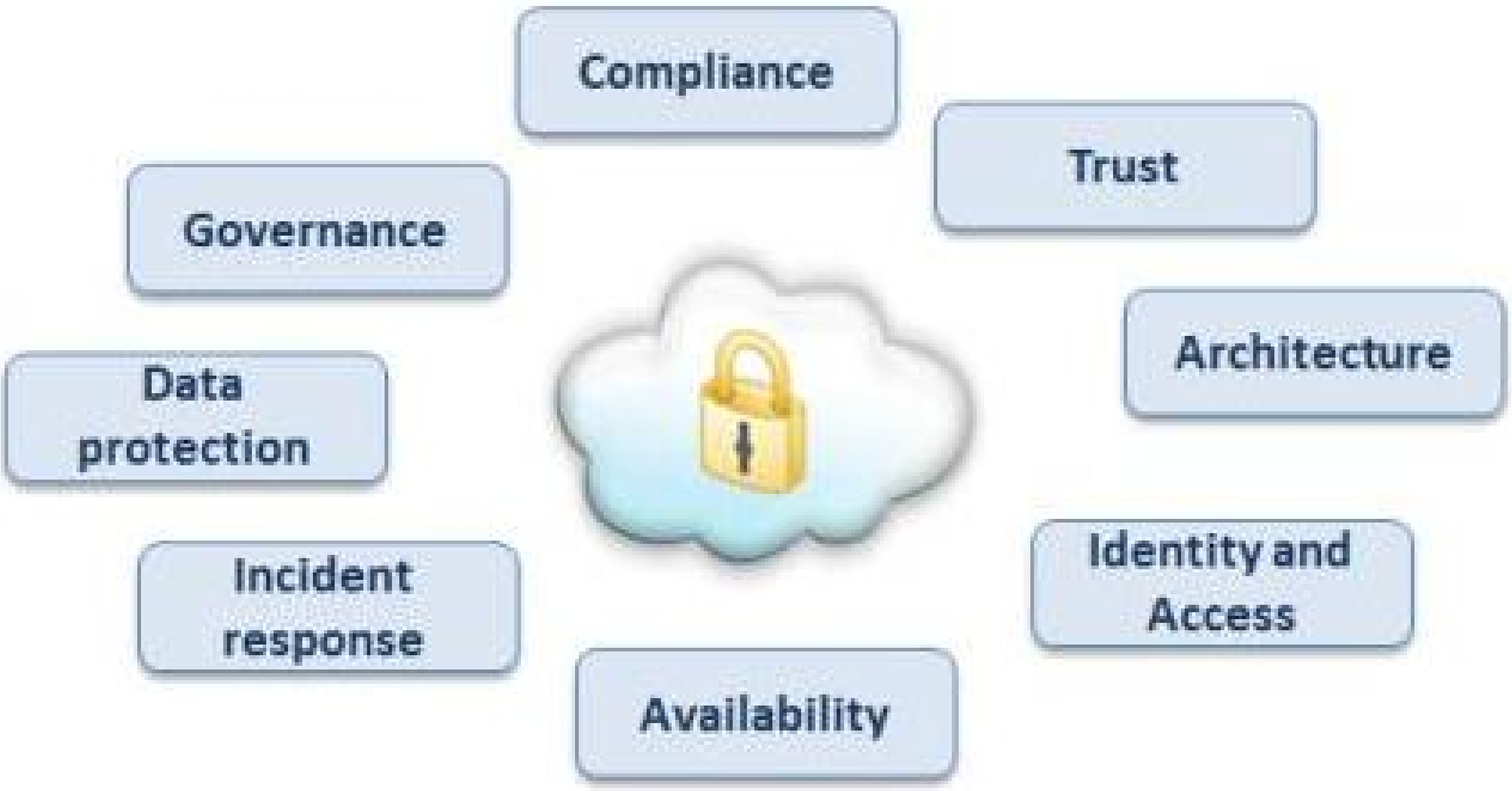
#2 – Cloud Services



#2 – Cloud Services



#2 – Cloud Services

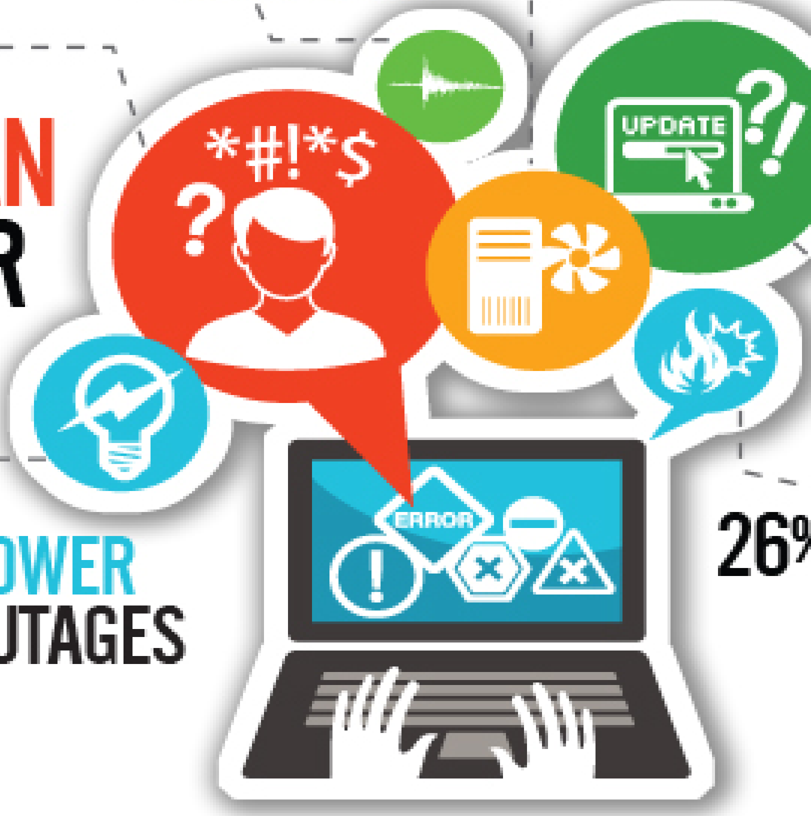


60% HUMAN ERROR

10% EARTHQUAKES

44% SERVER ROOM ISSUES

56% UNEXPECTED UPDATES & PATCHES

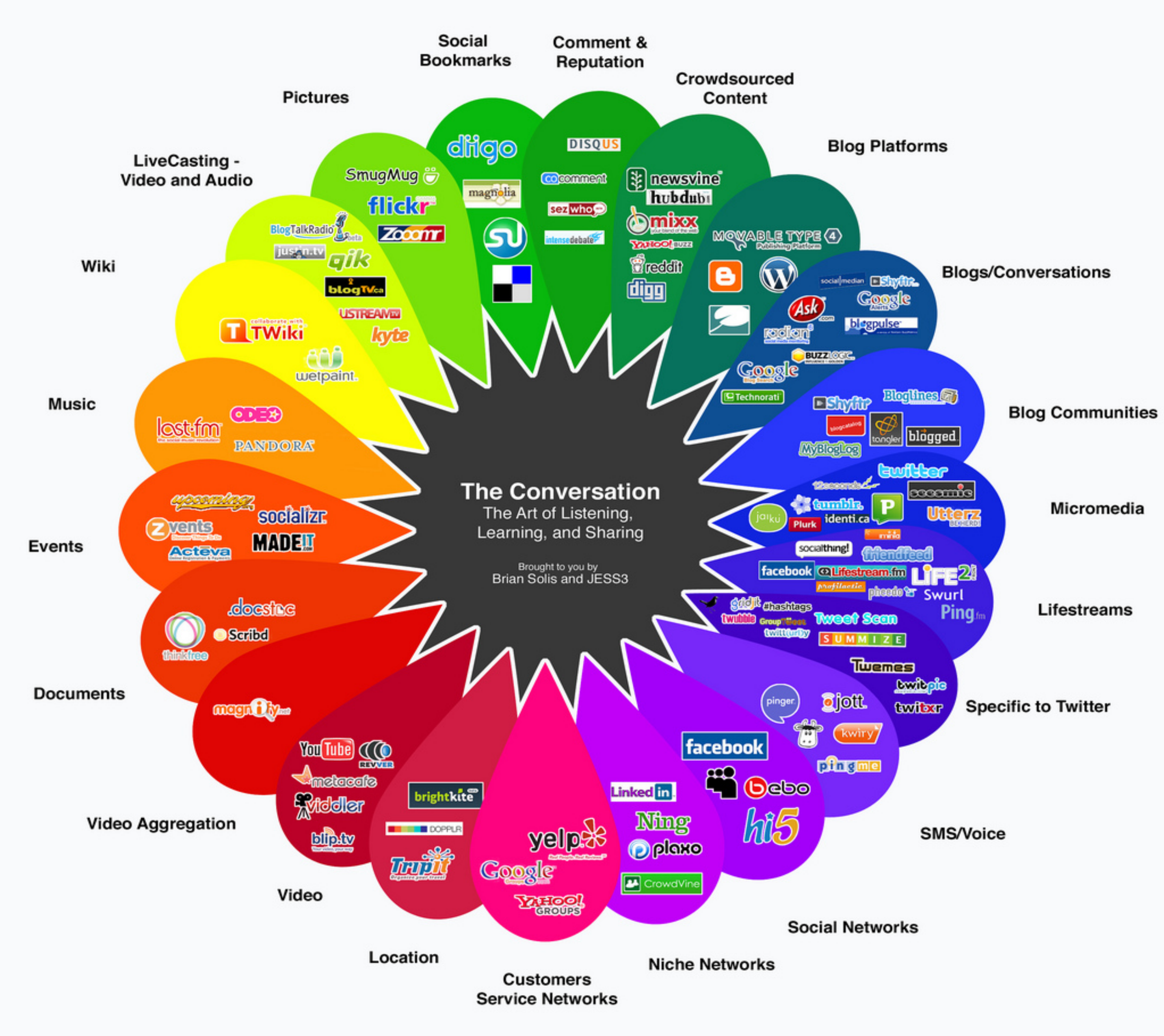


29% POWER OUTAGES

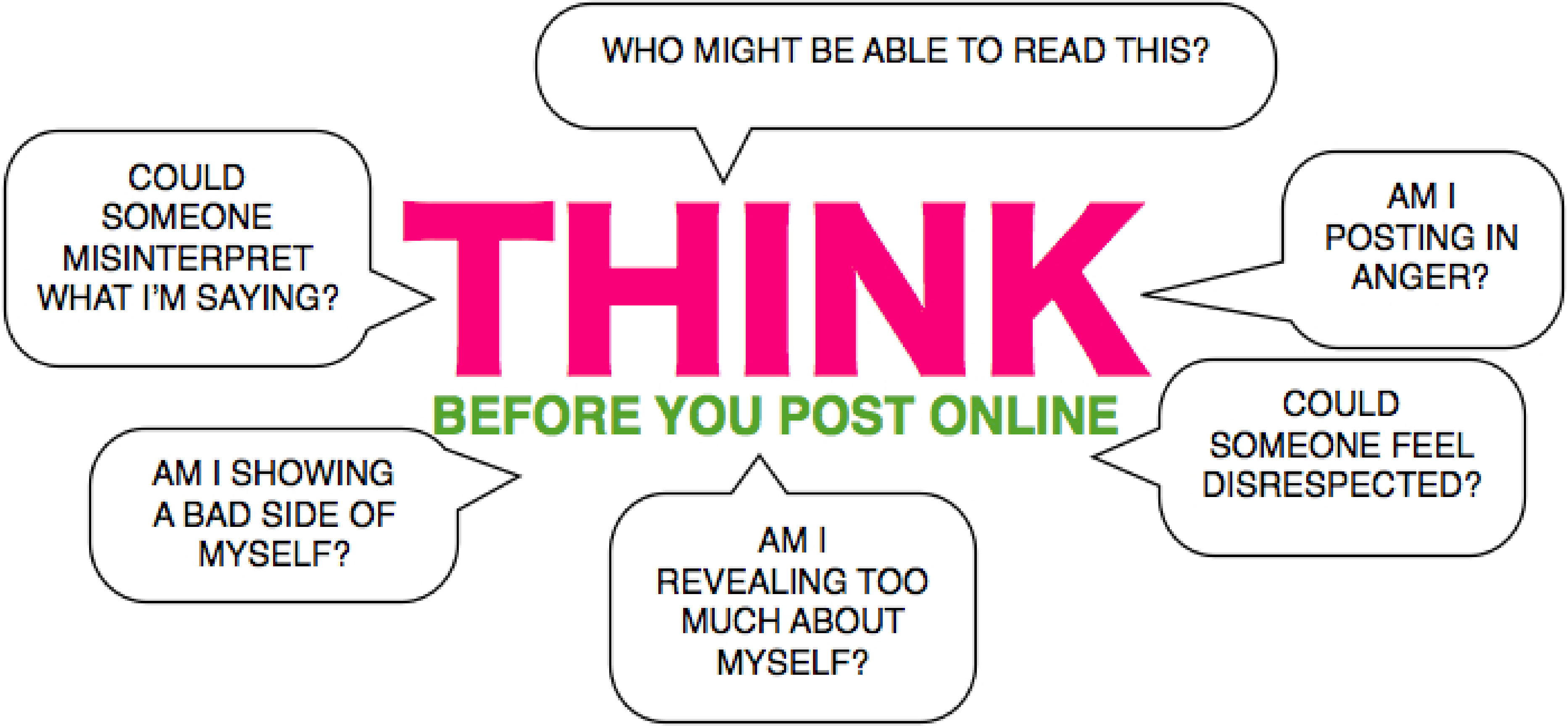
26% FIRE OR EXPLOSIONS

#2 – Social Media

Social Media Communication



facebook
Linked in
digg
Y
lost.fm
You Tube
orkut
SOCIAL MEDIA
In Business



THINK

BEFORE YOU POST ONLINE

WHO MIGHT BE ABLE TO READ THIS?

COULD SOMEONE MISINTERPRET WHAT I'M SAYING?

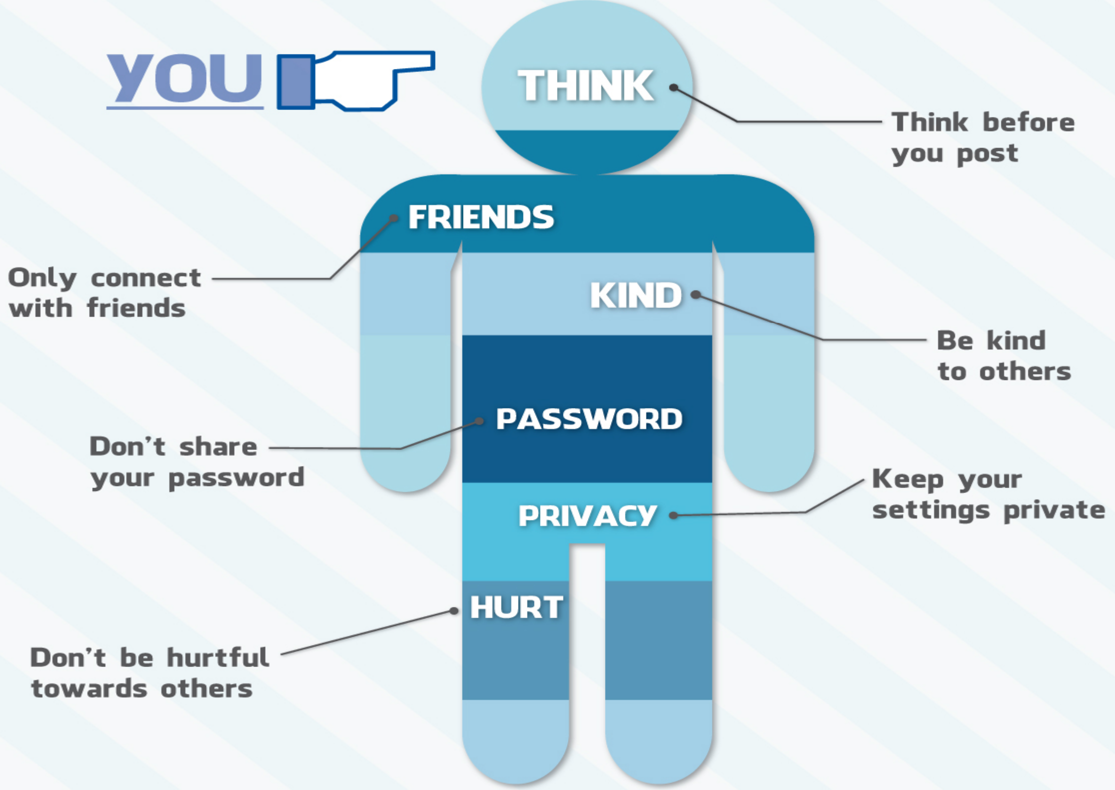
AM I POSTING IN ANGER?

COULD SOMEONE FEEL DISRESPECTED?

AM I SHOWING A BAD SIDE OF MYSELF?

AM I REVEALING TOO MUCH ABOUT MYSELF?

safebook



YOU

THINK

Think before you post

FRIENDS

Only connect with friends

KIND

Be kind to others

PASSWORD

Don't share your password

PRIVACY

Keep your settings private

HURT

Don't be hurtful towards others

PARENTS & TEACHERS

Join Facebook
Understand how it works
Teach safety and responsibility
Privacy – check their settings

FRIENDS

DON'T: Stay silent

DO: Help your friend
Report the bully
Tell your parents
Tell your teacher

THE BULLY

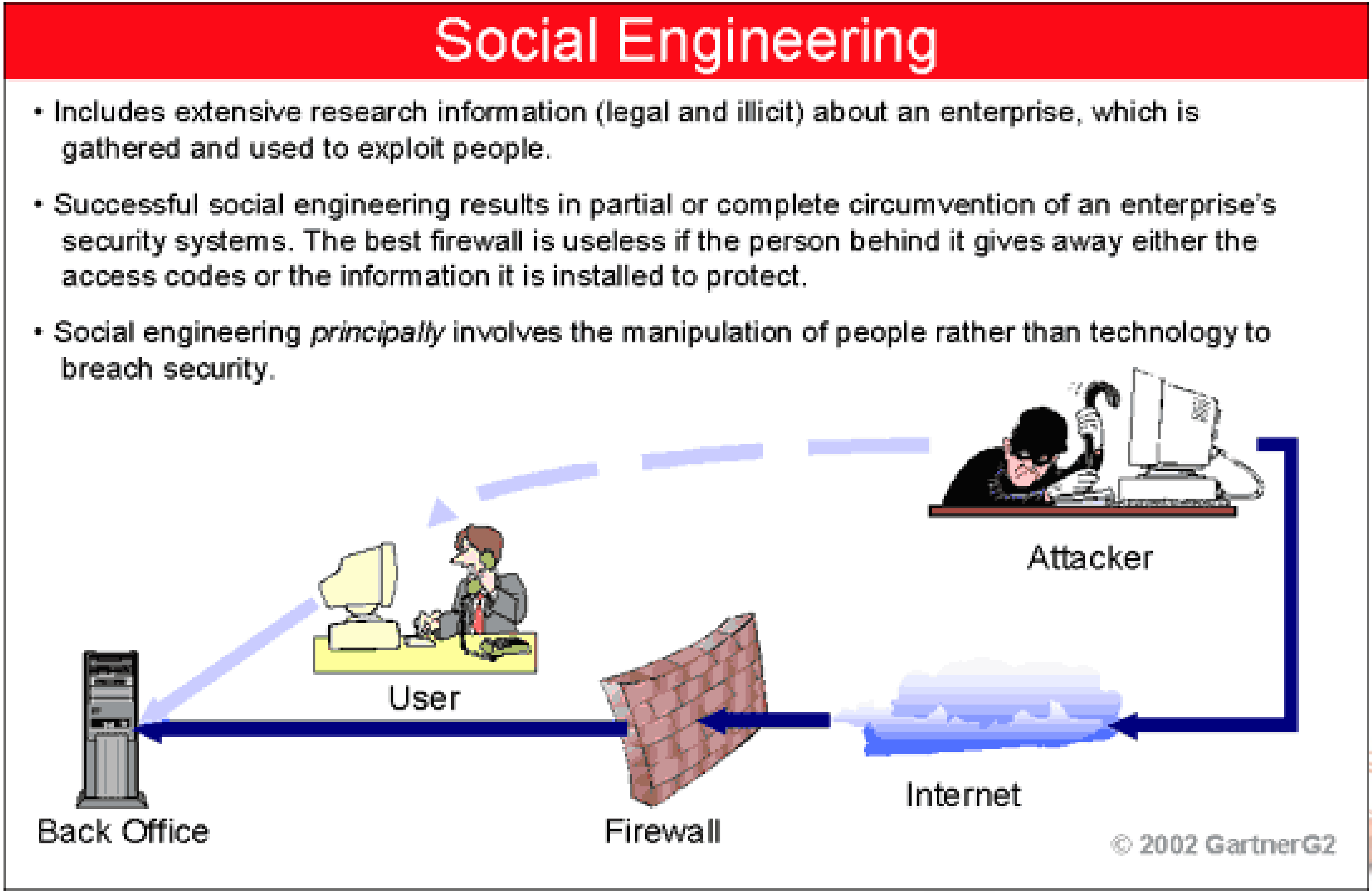
DON'T: Respond

DO: Save what they say
Unfriend the person
Block them
Tell a Friend
Tell your Parents
Report the person

TELL • UNFRIEND • BLOCK • REPORT

This is our reaction to cyber-bullying. We must all play our part! Play yours - email **design@fuzion.ie** for a print ready file

#5 – Social Engineering

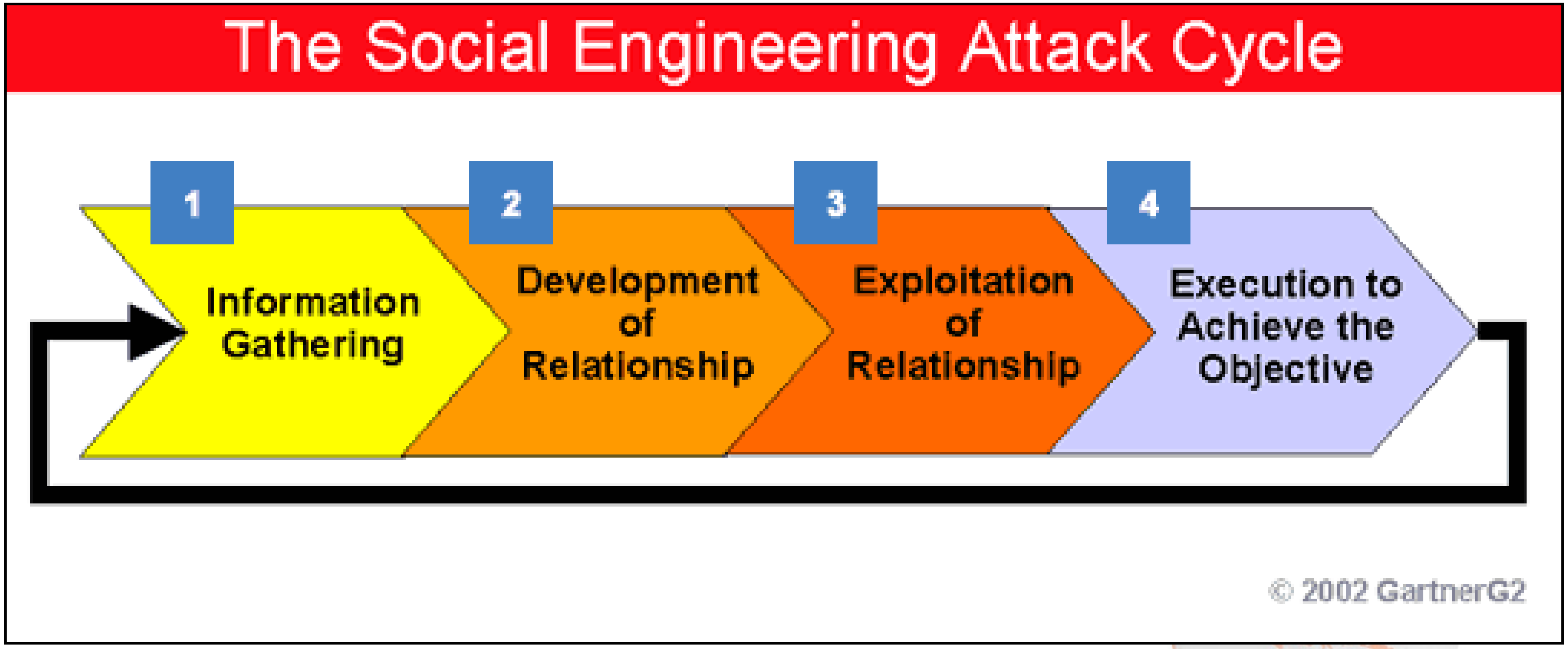


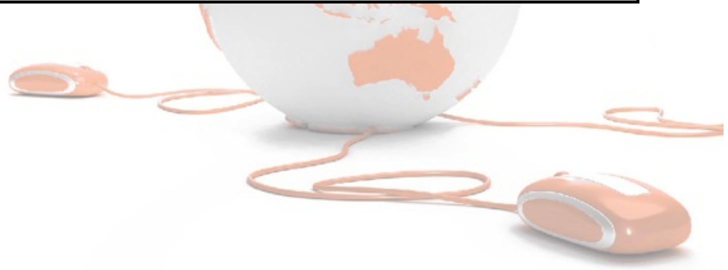
Social Engineering

- Includes extensive research information (legal and illicit) about an enterprise, which is gathered and used to exploit people.
- Successful social engineering results in partial or complete circumvention of an enterprise's security systems. The best firewall is useless if the person behind it gives away either the access codes or the information it is installed to protect.
- Social engineering *principally* involves the manipulation of people rather than technology to breach security.

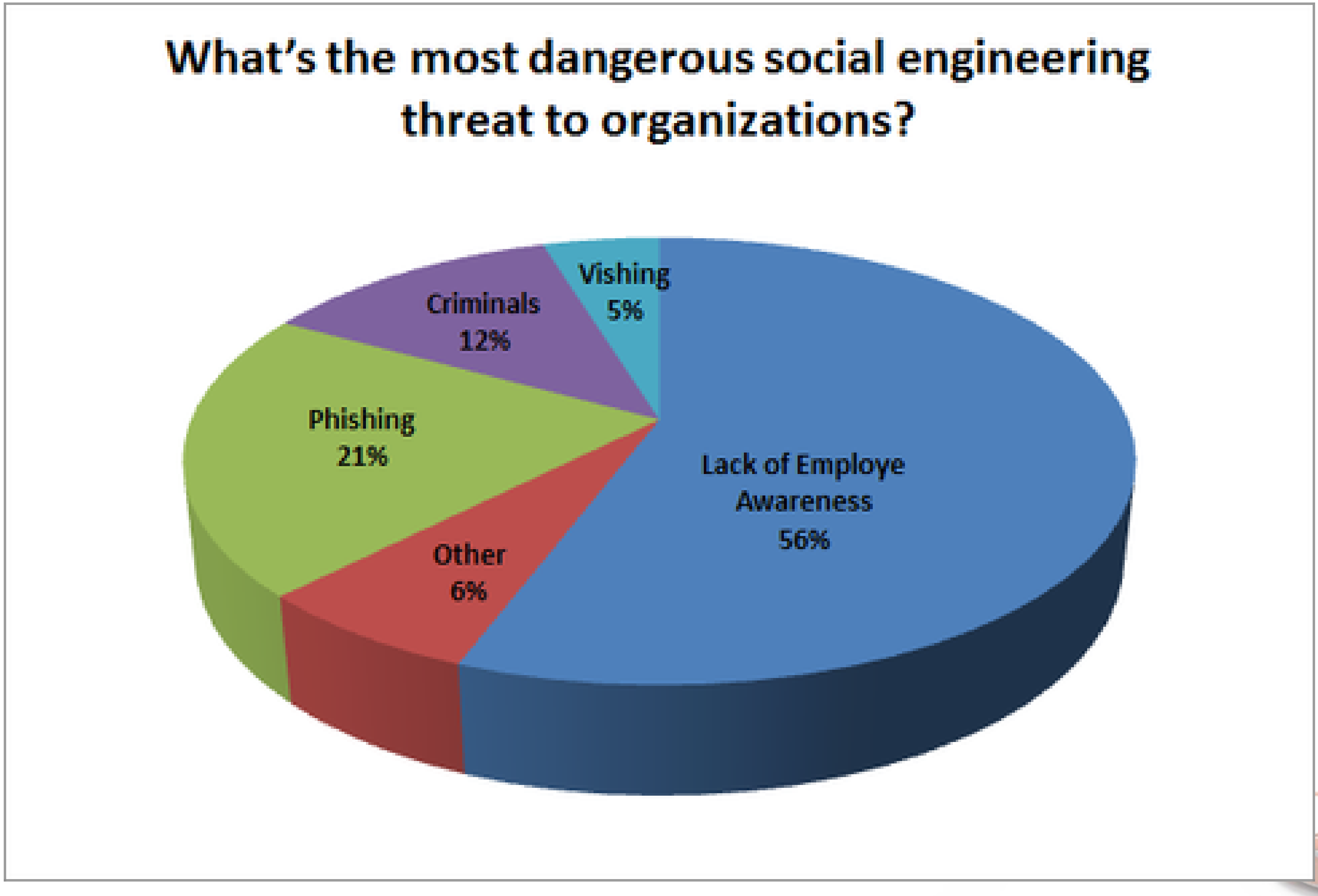
© 2002 GartnerG2

#5 – Social Engineering

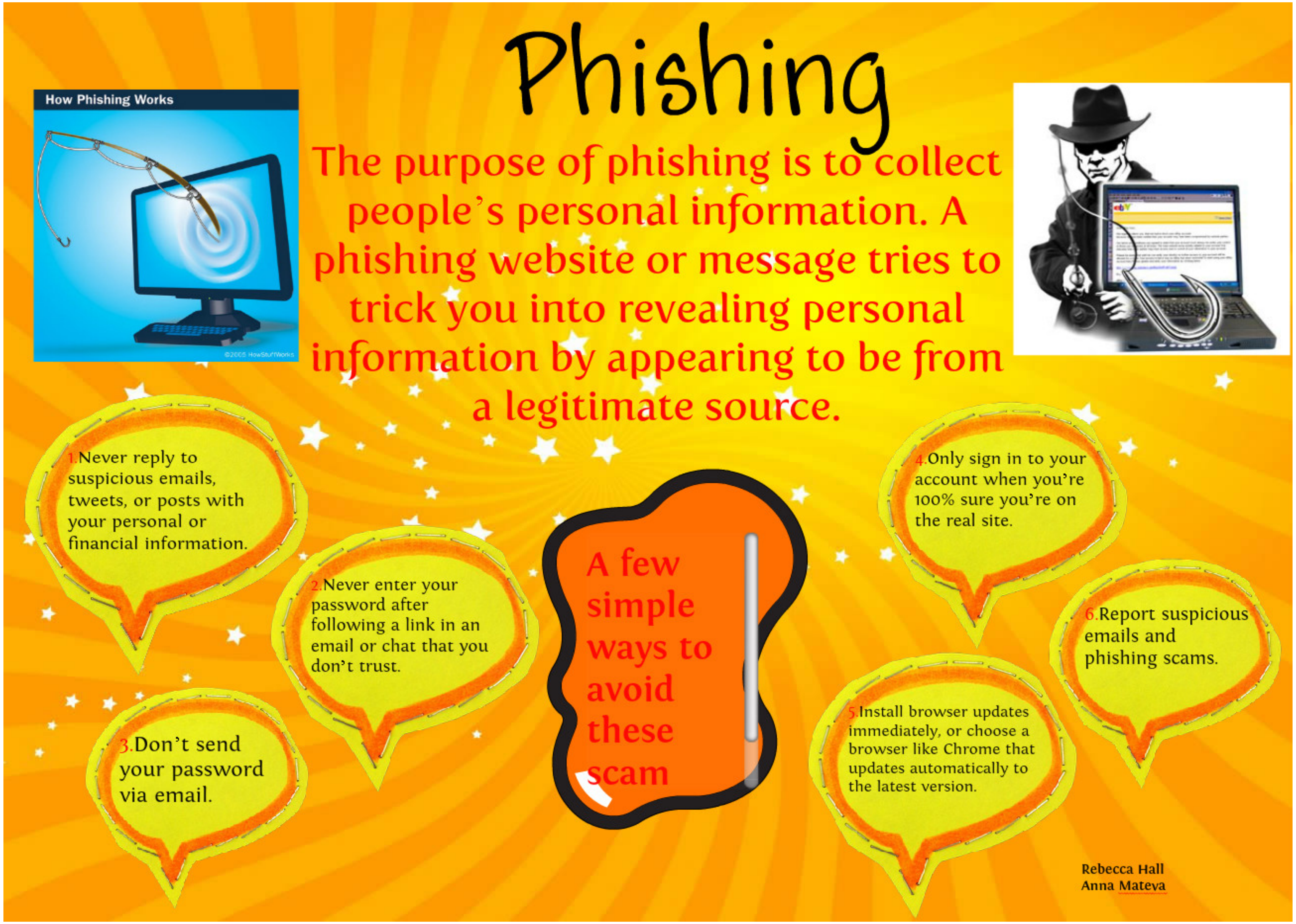

The Social Engineering Attack Cycle
1
Information Gathering
2
Development of Relationship
3
Exploitation of Relationship
4
Execution to Achieve the Objective
© 2002 GartnerG2



#5 – Social Engineering



#6 – Phishing



How Phishing Works

©2005 HowStuffWorks

Phishing

The purpose of phishing is to collect people's personal information. A phishing website or message tries to trick you into revealing personal information by appearing to be from a legitimate source.

A few simple ways to avoid these scam

1.Never reply to suspicious emails, tweets, or posts with your personal or financial information.

2.Never enter your password after following a link in an email or chat that you don't trust.

3.Don't send your password via email.

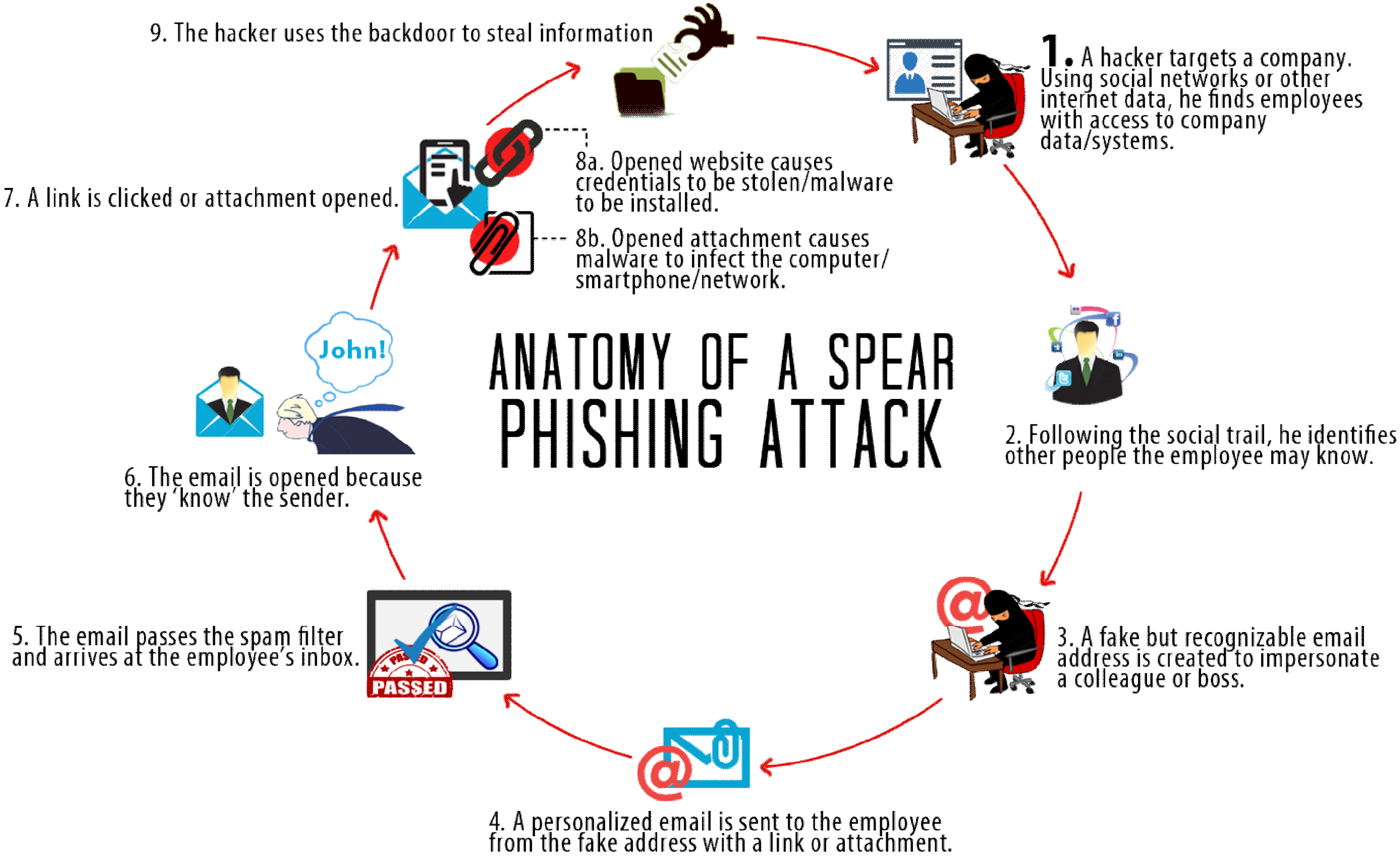
4.Only sign in to your account when you're 100% sure you're on the real site.

5.Install browser updates immediately, or choose a browser like Chrome that updates automatically to the latest version.

6.Report suspicious emails and phishing scams.

Rebecca Hall
Anna Mateva

#6 – Phishing



ANATOMY OF A SPEAR PHISHING ATTACK

1. A hacker targets a company. Using social networks or other internet data, he finds employees with access to company data/systems.

2. Following the social trail, he identifies other people the employee may know.

3. A fake but recognizable email address is created to impersonate a colleague or boss.

4. A personalized email is sent to the employee from the fake address with a link or attachment.

5. The email passes the spam filter and arrives at the employee's inbox.

6. The email is opened because they 'know' the sender.

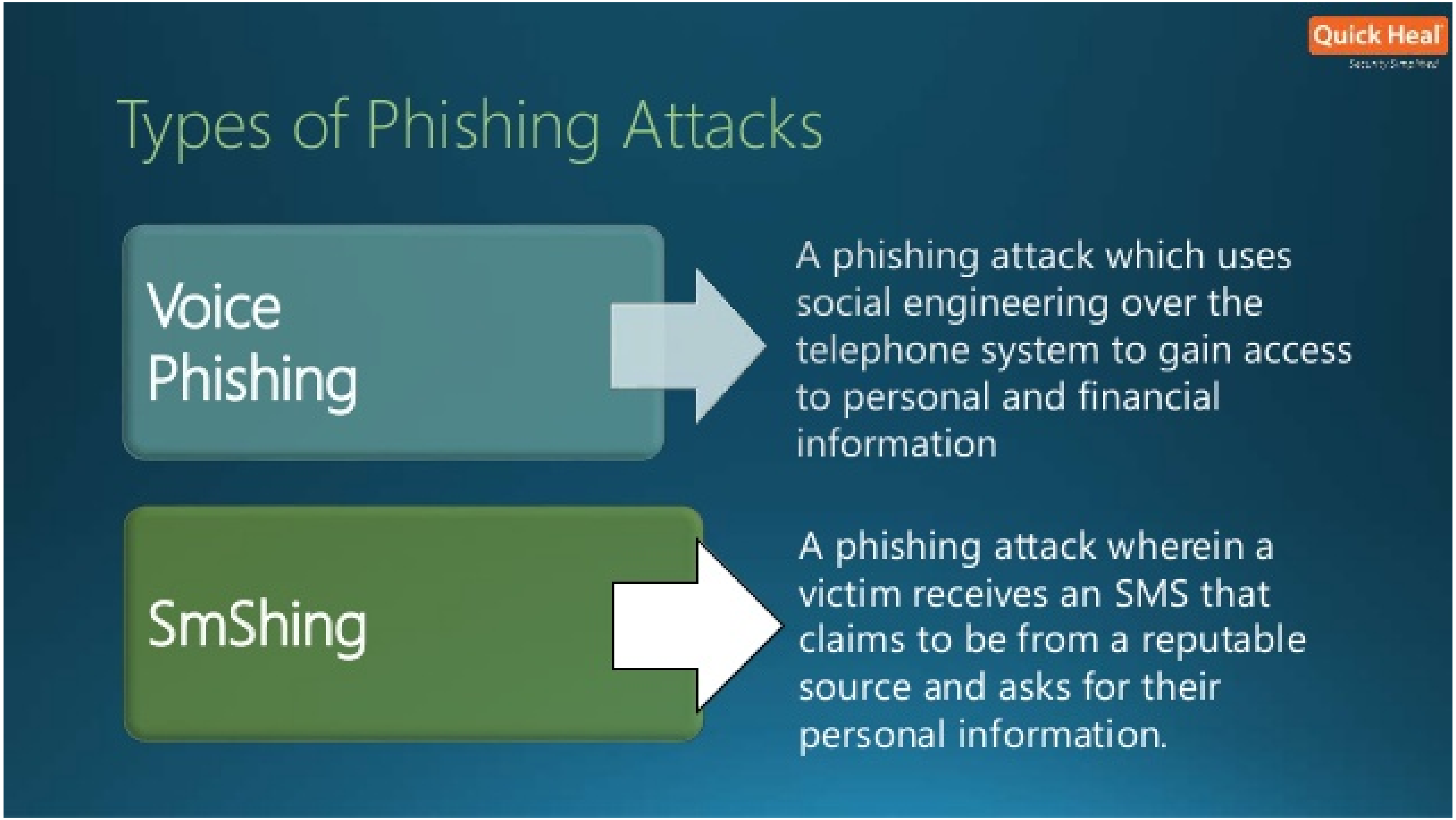
7. A link is clicked or attachment opened.

8a. Opened website causes credentials to be stolen/malware to be installed.

8b. Opened attachment causes malware to infect the computer/ smartphone/network.

9. The hacker uses the backdoor to steal information

#7 – Vshing & SMShing



Quick Heal
Security Simplified

Types of Phishing Attacks

Voice Phishing → A phishing attack which uses social engineering over the telephone system to gain access to personal and financial information

SmShing → A phishing attack wherein a victim receives an SMS that claims to be from a reputable source and asks for their personal information.

Don’t Phish Me

MyCERT

Malaysia Computer Emergency Response Team

End Message

Cyber Security

is everyone's responsibility...

Protect your information

at home and at work!

THANK YOU
for listening

Jazannul Azriq Aripin

Senior Executive Outreach,
CyberSecurity Malaysia

Email	**:**	**azriq@cybersecurity.my**
website	**:**	**www.cybersafe.my**
inquiry	**:**	**cybersafe@cybersecurity.my**
reporting	**:**	**cyber999@cybersecurity.my**

KEMENTERIAN SAINS, TEKNOLOGI DAN INOVASI
MINISTRY OF SCIENCE, TECHNOLOGY AND INNOVATION

CyberSecurity MALAYSIA
An agency under MOSTI

Thank you

Corporate Office
CyberSecurity Malaysia,
Level 5, Sapura@Mines
No. 7 Jalan Tasik
The Mines Resort City
43300 Seri Kembangan
Selangor Darul Ehsan, Malaysia.

T : +603 8992 6888
F : +603 8992 6841
H : +61 300 88 2999

www.cybersecurity.my
info@cybersecurity.my

Northern Regional Office
CyberSecurity Malaysia,
Level 19, Perak Techno-Trade Centre
Bandar Meru Raya, Off Jalan Jelapang
30020 Ipoh, Perak Darul Ridzuan, Malaysia

T: +605 528 2088
F: +605 528 1905

www.facebook.com/CyberSecurityMalaysia
twitter.com/cybersecuritymy
www.youtube.com/cybersecuritymy

Best Brand Internet Security 2008 & 2009

CERTIFIED TO ISO/IEC 27001:2005
CERT NO. : AR4656

MS ISO/IEC 17025 TESTING
SAMM NO. 456
(MySEF LABORATORY)

MSC MALAYSIA Status Company

Best Child Online Protection Website