“Cyber Security”

By

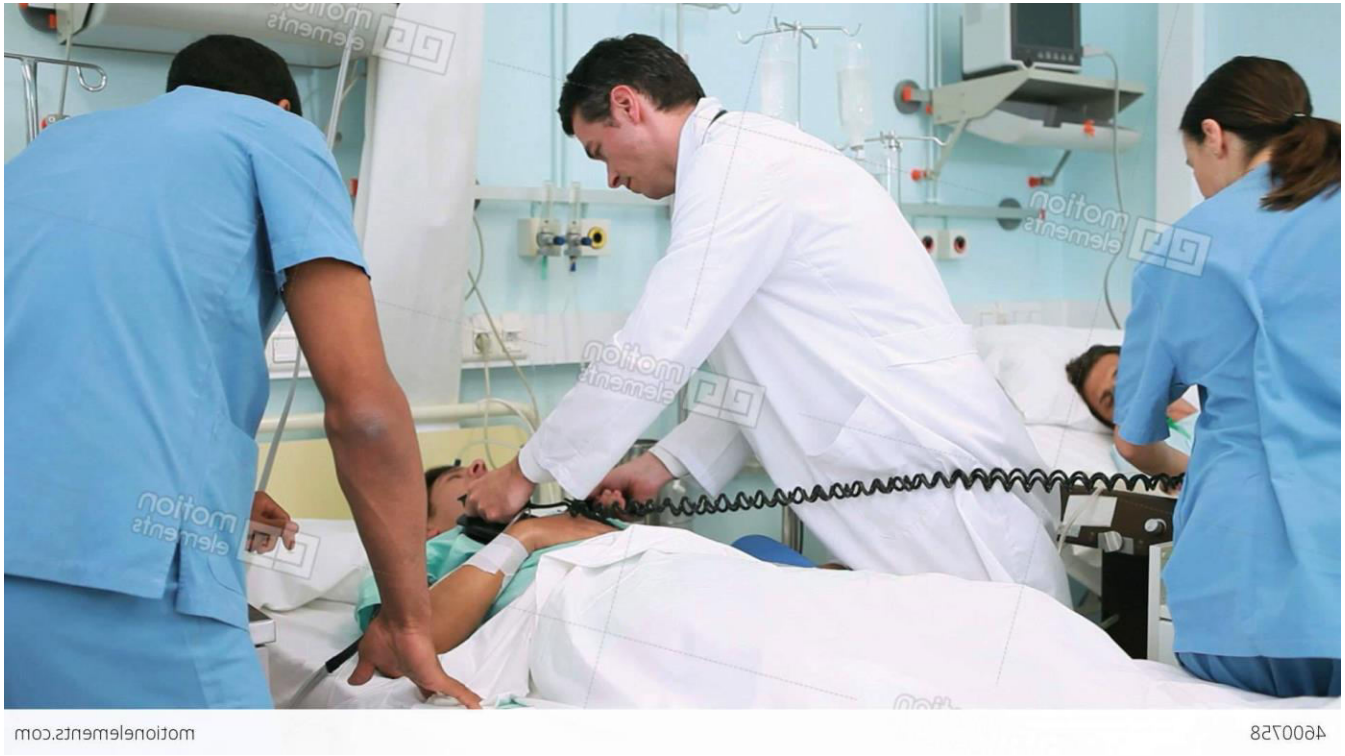
Dr. SUDALAIMUTHU T.

Associate Professor, Department of Computer Science and Engineering
Hindustan University, Chennai, India

Knowledge Vs Common Sense

Wife admitted her husband in the Hospital unconsciously

Knowledge Vs Common Sense



Doctors did so many tests and diagnostics

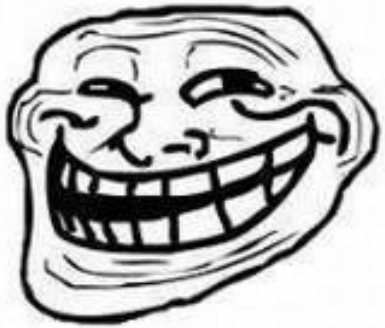
Knowledge Vs Common Sense

Doctor told wife, I am sorry, Your husband is no more.

Knowledge Vs Common Sense

But, the Husband stood up and said, "Doctor, I am live, Don't lie"

Wife replied, "Doctor knows better than you, Just keep quite, You died"



What we learnt in our class : Sun rises in the east and sets in the west.

Please! Its the earth which rotates not the sun rising or setting.!

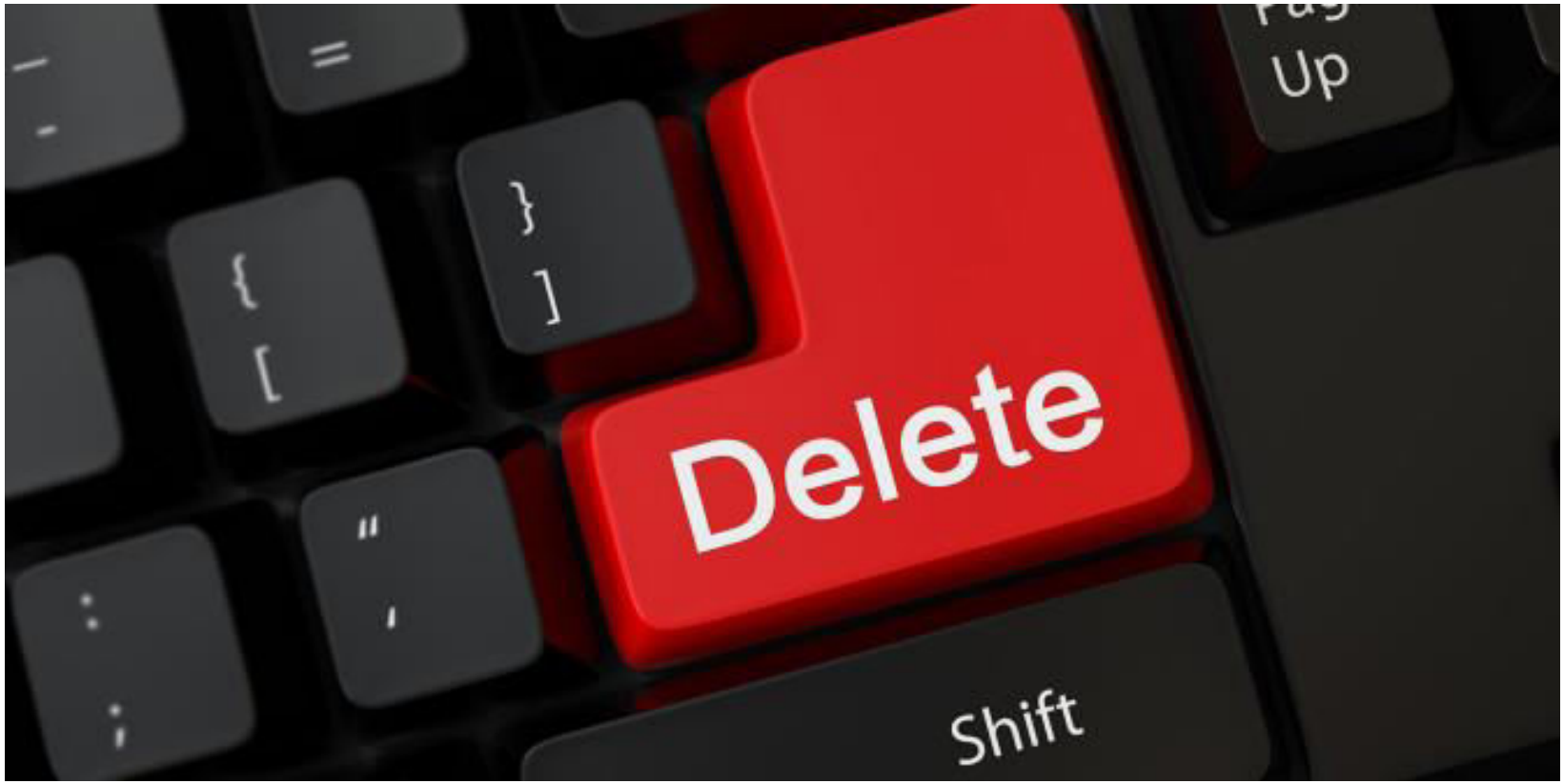
THATS TRUE !

Moral : Educatin spoils common sense!

PROBLEM??

Distributed by: Mememderp.com

File Deletion in a Computer

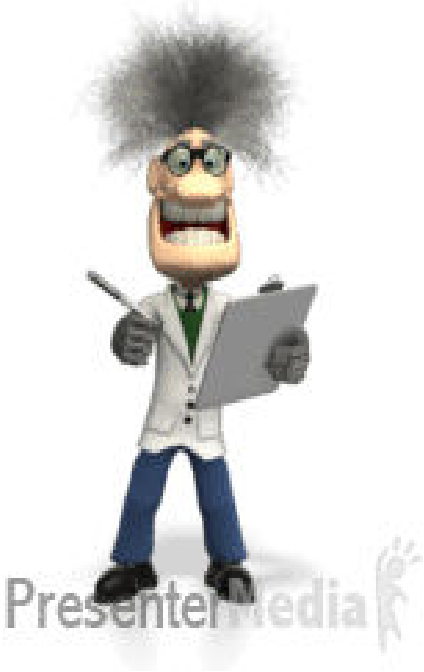


A Scientist & Frog

There once was a scientist who studied frogs. One day, the scientist put the frog on the ground and told it to jump. The frog jumped four feet.

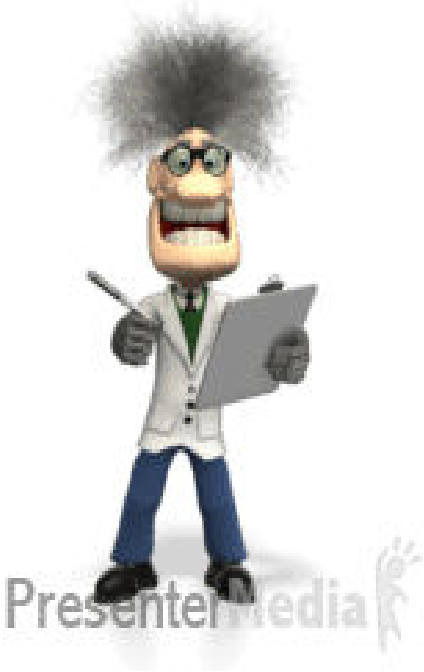
So the scientist wrote in his notebook, "Frog with four feet, jumps four feet."

A Scientist & Frog



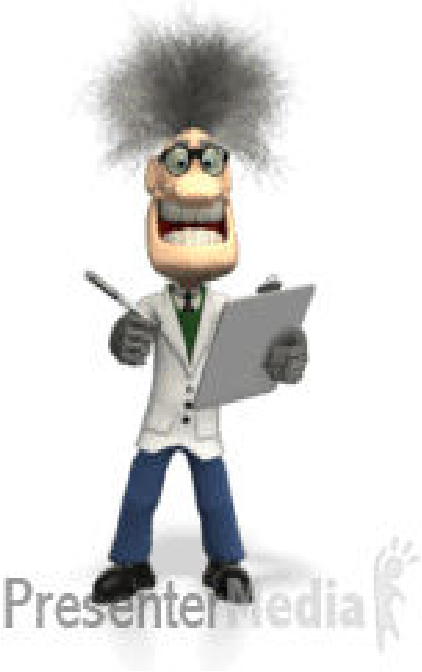
So the scientist cut off one of the frogs legs and told the frog to jump. Frog jumped three feet. The scientist wrote in his note book, "Frog with three legs, jumps three feet."

A Scientist & Frog



The scientist cut another leg and told the frog to jump. Frog jumped two feet. So the scientist wrote in his note book, "Frog with two legs, jumps two feet.“

A Scientist & Frog



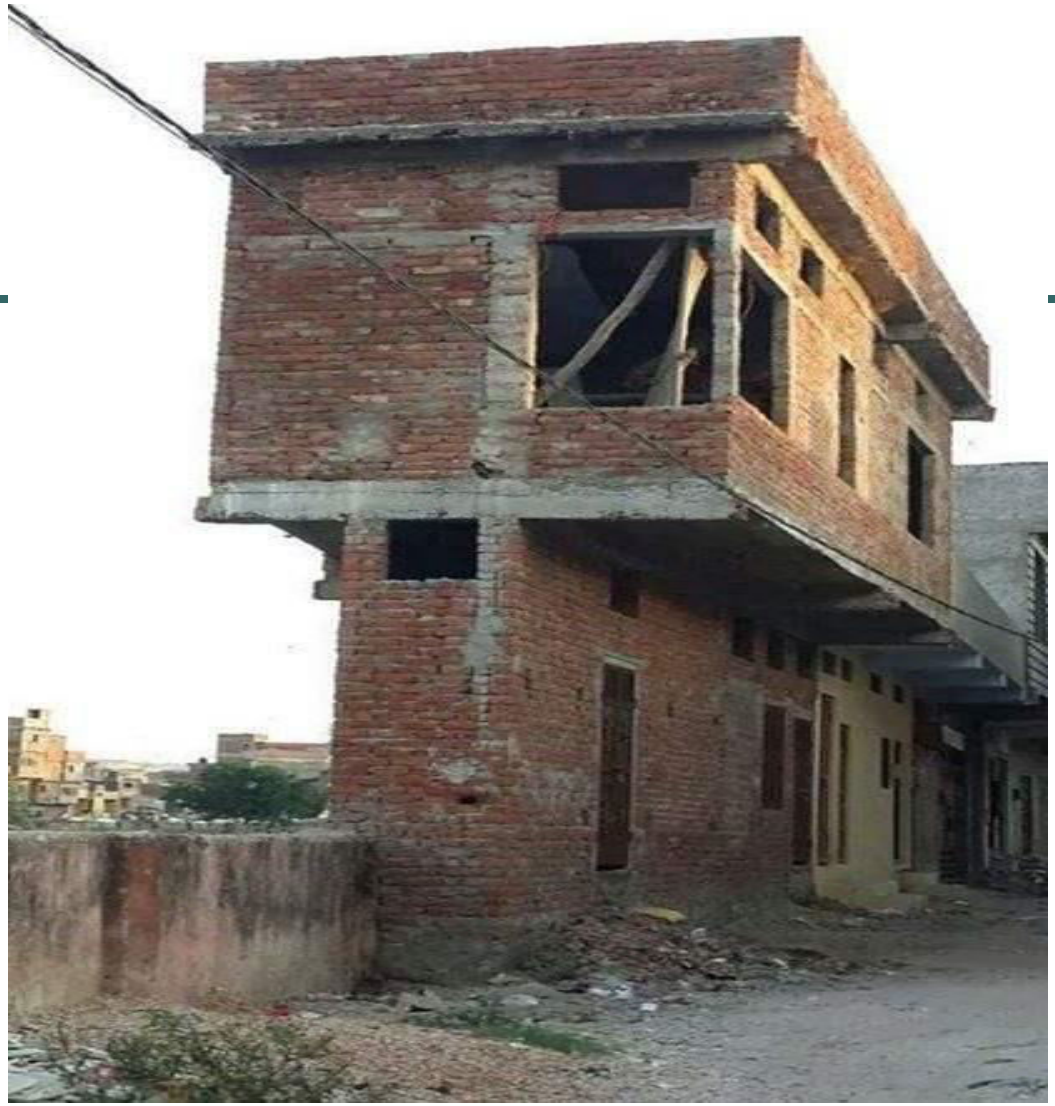
The scientist cut its last leg and told to jump. Frog not jumped.

The scientist wrote in his note book,

"Frog with no feet, goes deaf“

Lazy road worker didn't even have 1 second to take off that branch.

This highway engineer who didn't notice this huge tree.



An architectural job requires a lot of creativity and innovation. Here is the proof.

This architect who never attended a class during his diploma course.

This clockmaker who doesn't know how to count.

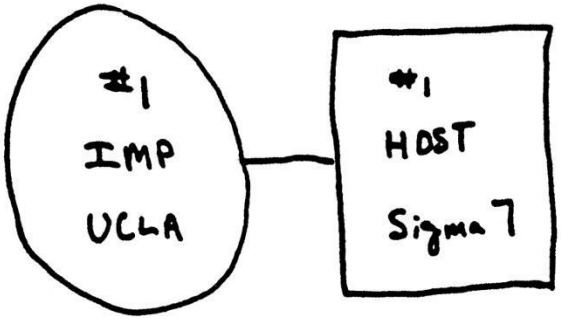
Did someone use a fake certificate to become an engineer.

Cyber Security is a Common Sense, than Knowledge. Why ?

To use Cyber Space

- *No Degree is required*
- *No Training is required*
- *No License is required*
- *No monitoring*
- *Use as you can model*
- *Anywhere any time*

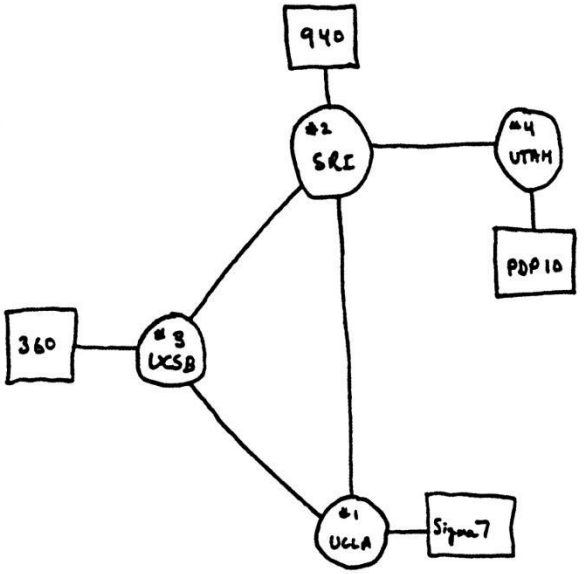
ARPA NET



THE ARPA NETWORK

SEPT 1969

1 NODE

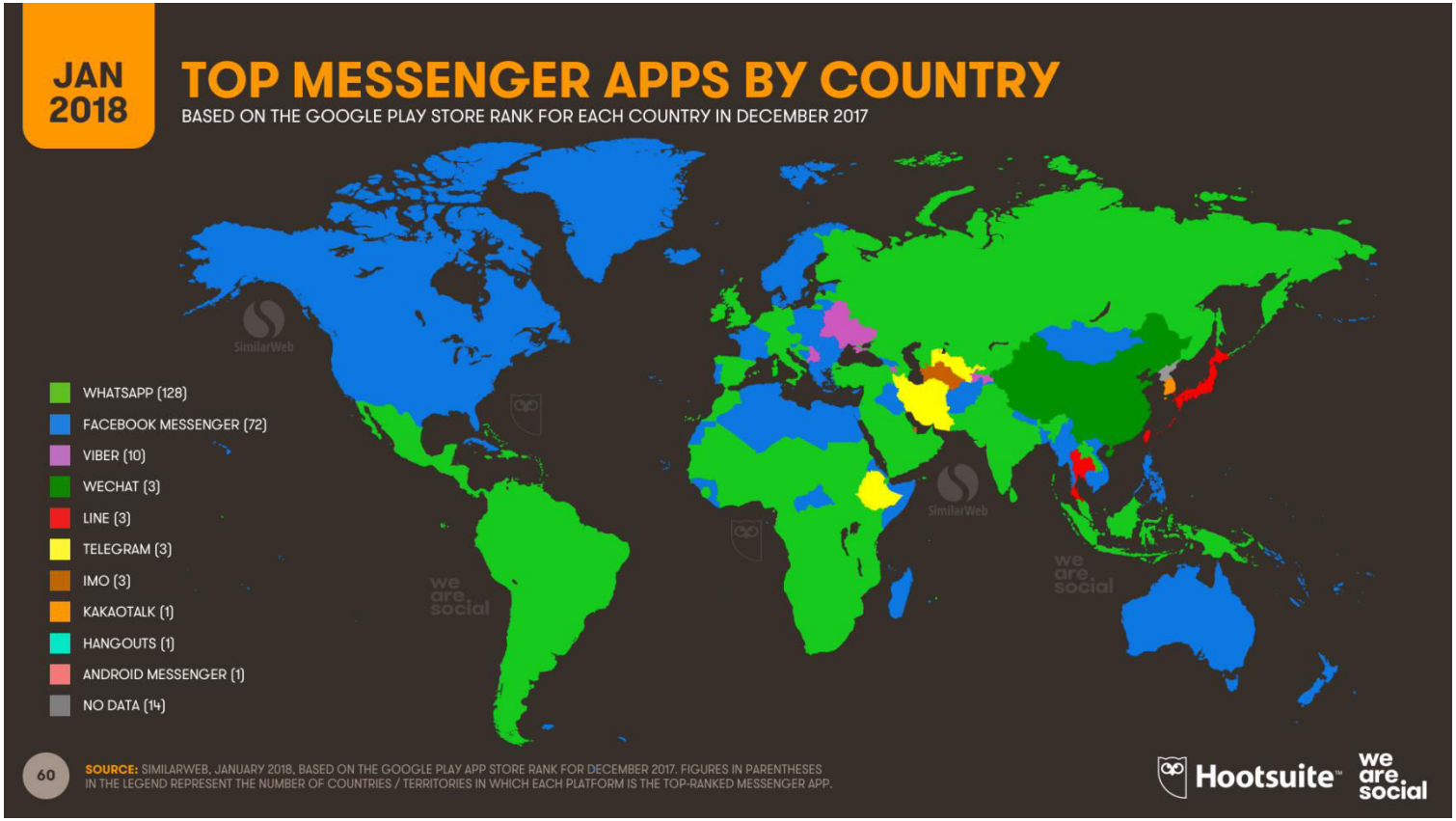


THE ARPA NETWORK

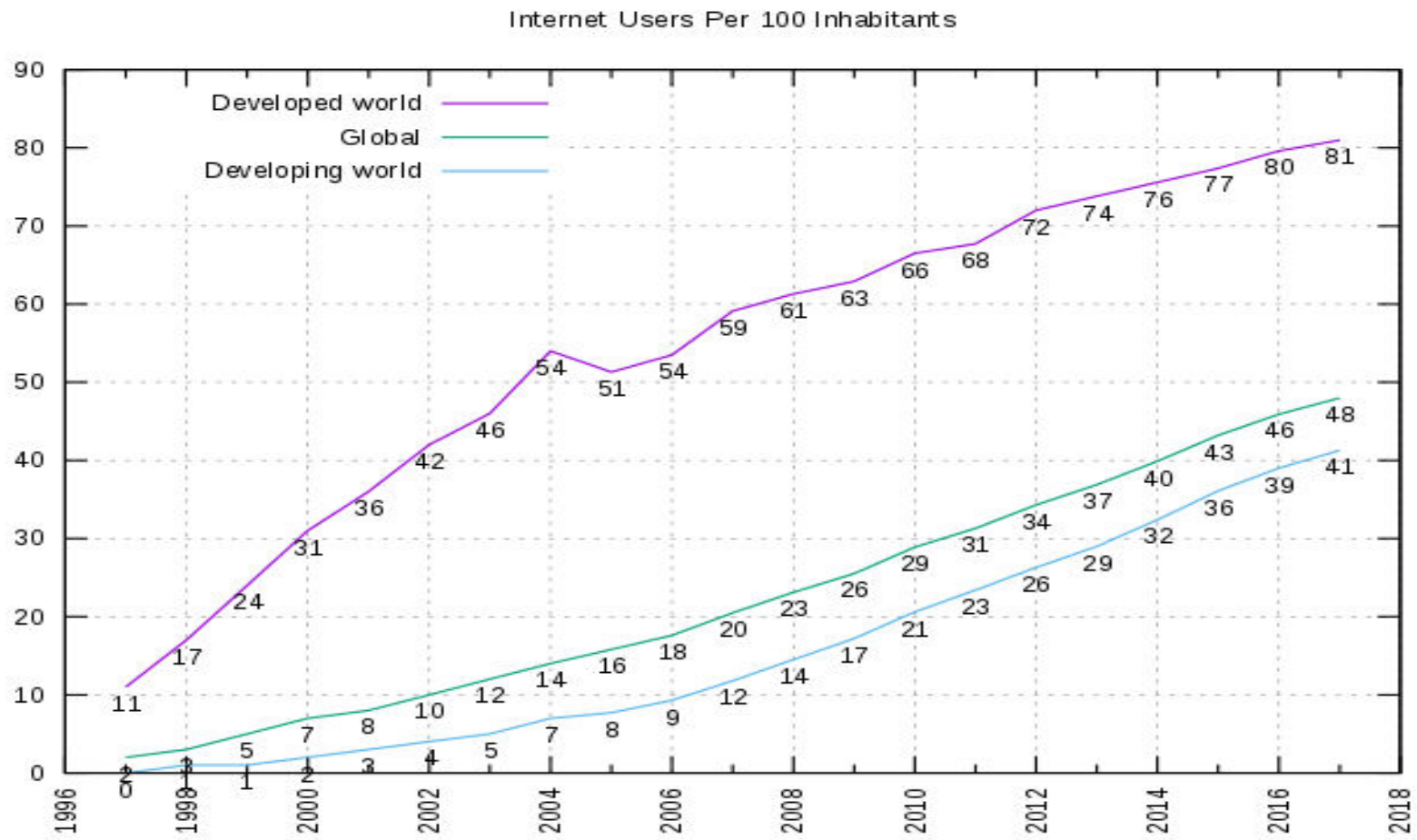
DEC 1969

4 NODES

Today Internet - APPS USAGE



INTERNET USAGE



Introduction – Cyber Security

- *Cyber-safety is a common term used to describe a set of practices, measures and/or actions you can take to protect personal information and your computer from attacks.*
- *Cyber safety threats*
  - *Viruses*
  - *Hackers*
  - *Identity Thieves*
  - *Spyware*

Two Groups of people in the Cyberspace

- 1. Known that they have been attacked
- 2. yet to know that they have been attacked

Cyber Attacks – Types - Passive

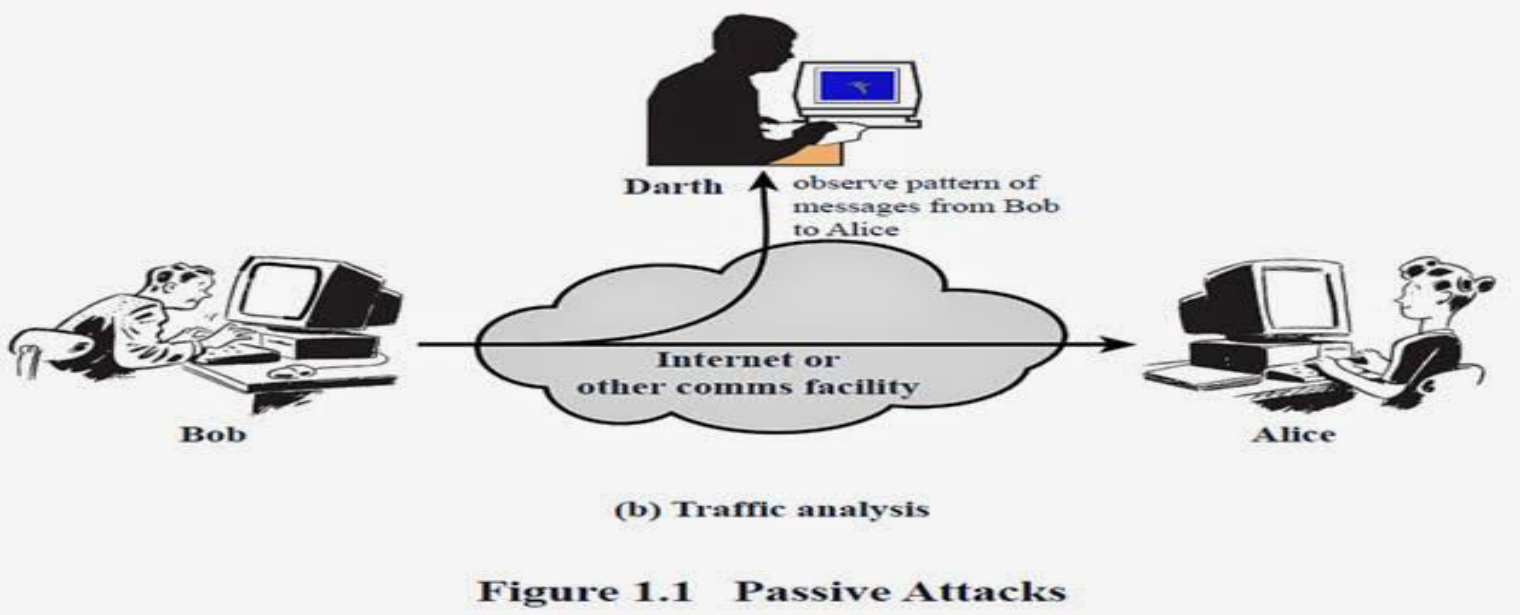
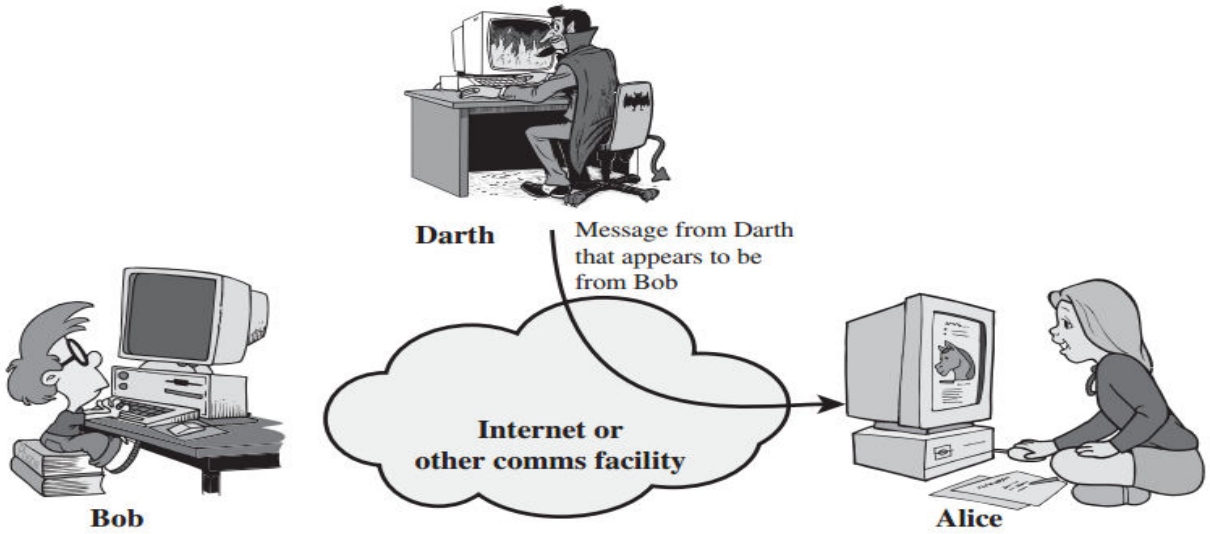


Figure 1.1 Passive Attacks

- attempts to learn or make use of information from the system but does not affect system resources
- examples: eavesdropping message contents, traffic analysis
- difficult to detect, should be prevented

Cyber Attacks – Types - Passive



- attempts to alter system resources or affect their operation
- examples: masquerade (spoofing), replay, modification (substitution, insertion, destruction), denial of service
- difficult to prevent, should be detected

Cyber Attack – C,I,A

- Confidentiality
  - Aims to protect data from unauthorized disclosure
  - Usually based on encryption
- Integrity
  - Aims to detect modification and replay
  - Provides assurance that data received are exactly as sent by the sender
- Access control
  - Aims to prevent unauthorized access to resources
- Authentication
  - Provides assurance that a communicating entity is the one that it claims to be
- Non-repudiation
  - provides protection against denial by one entity involved in a communication of having participated in all or part of the communication

Cyber safety threats

Viruses

Viruses infect computers through email attachments and file sharing. They delete files, attack other computers, and make your computer run slowly. One infected computer can cause problems for all computers on a network.

Hackers

Hackers are people who “trespass” into your computer from a remote location. They may use your computer to send spam or viruses, host a Web site, or do other activities that cause computer malfunctions.

Identity Thieves

People who obtain unauthorized access to your personal information, such as Social Security and financial account numbers. They then use this information to commit crimes such as fraud or theft.

Spyware

Spyware is software that “piggybacks” on programs you download, gathers information about your online habits, and transmits personal information without your knowledge. It may also cause a wide range of other computer malfunctions.

What is a Computer Virus?

- A computer virus is a computer program that can copy itself and infect a computer without the permission or knowledge of the owner.
- One of the first detected virus was the Creeper virus in the early 70's
- Before computer networks became widespread, most viruses spread on removable media, particularly floppy disk.

Basic Computer Viruses

- Trojan Horses
  - appears as interesting program file but when installed it allows intruders to access and read your files
- Worms
  - virus that copies and multiplies itself by using computer networks and security flaws
- E-mail Viruses
  - use e-mail messages to spread which allow it to automatically forward itself to thousands of people

Types of Viruses

- Boot Sector Virus
  - Infects the boot or MBR of diskettes and hard drives through the sharing of infected disks and pirated software applications
  - Once your hard drive is infected all diskettes that you use in your computer will be infected
- Program Virus
  - Becomes active when the program file (usually with extensions .BIN, .COM, .EXE, .OVL, .DRV) carrying the virus is opened
  - It then makes copies of itself and will infect other programs on the computer
- Multipartite Virus
  - Hybrid of a Boot Sector and Program viruses
  - It infects program files and when the infected program is active it will affect the boot record

Types of Viruses

- Stealth Virus
  - Disguises itself to prevent from being detected by antivirus software
  - It alters its file size or conceals itself in memory
- Polymorphic Virus
  - Act like a chameleon, changing its virus signature (binary pattern) every time it multiples and infects a new file
- Macro Virus
  - Programmed as a macro embedded in a document, usually found in Microsoft Word and Excel
  - Once it gets in to your computer, every document you produce will become infected
  - Relatively new type of virus and may slip by your antivirus software if you don't have the most recent version installed

Signs Your Computer is Infected

- Functions slower than normal
- Responds slowly and freezes often
- Restarts itself often
- See uncommon error messages, distorted menus, and dialog boxes
- Notice applications fail to work correctly
- Fail to print correctly

Impact of Virus

Loss of access to the campus computing network

Loss of confidentiality, integrity and/or availability of valuable university information, research and/or personal electronic data

Lawsuits, loss of public trust and/or grant opportunities, prosecution, internal disciplinary action or termination of employment

How to write a Virus ?

- Only Experts can write a virus ?
- Specific Task to do
- Memory Usage
- Service Usage
- Computing Usage
- Confusion in Decision

Confusion in Decision - Virus

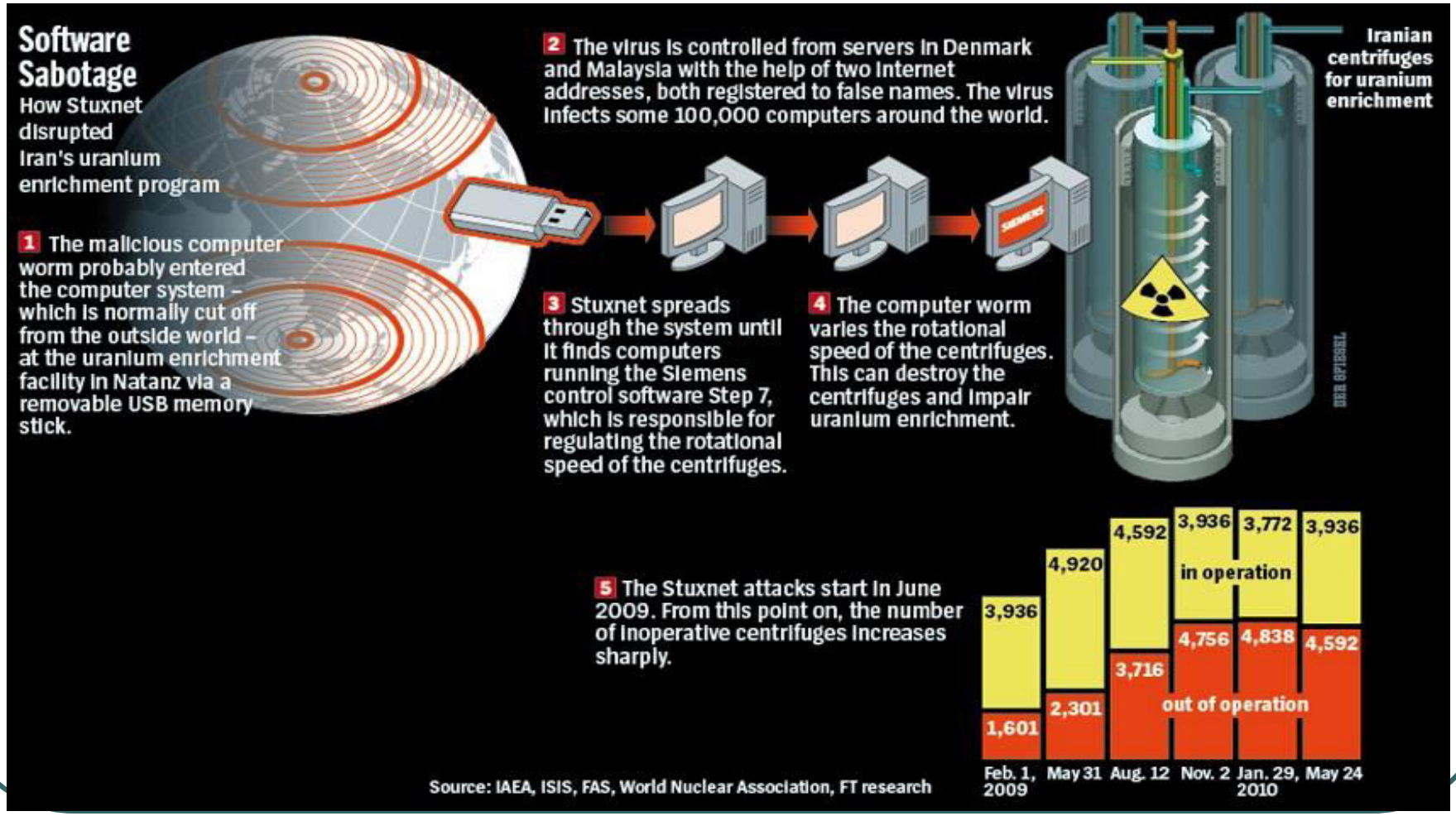
- The anger King asked his minister to tell any statement,
- If the statement is true then he will be killed by hanged
- Else if false, then he will be killed by poison.
- How do you escape ?

- “You are going to kill me by Poison”

Cyber Security - State of the Art

Who needs a gun when you have a keyboard?

Stuxnet – Iran Nuclear Project



Cyber Security - State of the Art

MafiaBoy causes $1 billion dollars in damages (2000):

- ***DDoS attack on a number of high-profile commercial websites including Amazon, CNN, eBay***
- ***An industry expert estimated the attacks resulted in a $US1.2 billion dollar damage bill.***

Cyber Security - State of the Art

Google China hit by cyber attack (2009):

- ***When Google's Chinese headquarters detected a security breech in mid-December, it opened up a whole can of worms (pun intended) implicating the Chinese Government.***
- ***Hackers had gained access to several Google's corporate servers and intellectual property was stolen.***

Cyber Security - State of the Art

Teen hacks NASA and US Defense Department:

- ***James had managed to penetrate the computers of a Defense , US., and installed a 'backdoor'. This allowed him to intercept thousands of internal emails.***
- ***Using the stolen information, James was able to steal a piece of NASA software which cost the space exploration agency $41,000 as systems were shutdown for three weeks. .***

Cyber Security - State of the Art

The Melissa virus (1999)

- ***It was a very simple virus which ended up costing $80 million in damages.***

  The Melissa virus would infect Microsoft Word documents and automatically disseminates itself as an attachment via email. It would mail out to the first 50 names listed in an infected computer's Outlook email address box.

Cyber Security - State of the Art

Hacker steals tens of million of credit card details

- ***Gonzales, a hacker from Miami, was responsible for one of the biggest fraud case in US history.***

  Gonzales was responsible for sealing tens of millions of credit card and debit card numbers from over 250 financial institutions. He had hacked the payment card network from companies including the 7-Eleven convenient store chain.

Some types of Cyber Threats

Type	Motivation	Target	Method
Information Warfare	Military or political dominance	Critical infrastructure, political and military assets	Attack, corrupt, exploit, deny, conjoint with physical attack
Cyber Espionage	Gain of intellectual Property and Secrets	Governments, companies, individuals	Advanced Persistent Threats
Cyber Crime	Economic gain	Individuals, companies, governments	Fraud, ID theft, extortion, Attack, Exploit
Cracking	Ego, personal enmity	Individuals, companies, governments	Attack, Exploit
Hactivism	Political change	Governments, Companeis	Attack, defacing
Cyber Terror	Political change	Innocent victims, recruiting	Marketing, command and control, computer based voilence

Source: analysis, Dr Irv Lachov

OWASP Top 10 Security Vulnerabilities

- 1 - Cross Site Scripting (XSS) XSS flaws occur whenever an application takes user supplied data and sends it to a web browser without first validating.
- 2 - Injection Flaws Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query.
- 3 - Malicious File Execution Code vulnerable to remote file inclusion (RFI) allows attackers to include hostile code and data, resulting in devastating attacks, such as total server compromise..
- 4 - Insecure Direct Object Reference A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, database record, or key, as a URL or form parameter.
- 5 - Cross Site Request Forgery (CSRF) A CSRF attack forces a logged-on victim's browser to send a pre-authenticated request to a vulnerable web application, which then forces the victim's browser to perform a hostile action to the benefit of the attacker.

OWASP Top 10 Security Vulnerabilities

- **6 - Information Leakage and Improper Error Handling** Applications can unintentionally leak information about their configuration, internal workings, or violate privacy through a variety of application problems. Attackers use this weakness to steal sensitive data, or conduct more serious attacks.
- **7 - Broken Authentication and Session Management** Account credentials and session tokens are often not properly protected. Attackers compromise passwords, keys, or authentication tokens to assume other users' identities.
- **8 - Insecure Cryptographic Storage** Web applications rarely use cryptographic functions properly to protect data and credentials. Attackers use weakly protected data to conduct identity theft and other crimes, such as credit card fraud.
- **9 - Insecure Communications** Applications frequently fail to encrypt network traffic when it is necessary to protect sensitive communications.
- **10 - Failure to Restrict URL Access** Frequently, an application only protects sensitive functionality by preventing the display of links or URLs to unauthorized users. Attackers can use this weakness to access and perform unauthorized operations by accessing those URLs directly.

OWASP Top 1: Cross Site Scripting

- What is Cross Site Scripting?
  - In it's simplest form, it's a process that can occur anywhere a web application uses input from a malicious user to generate output without validating or encoding the input.
  - During a Cross Site Scripting attack, a malicious source sends a script that is executed by the end user's browser. It allows attackers to embed code from one webpage into another webpage by changing its HTML code.
  - It's been used to deface web sites, conduct phishing attacks, or it can take over a user's browser and force them to execute commands they're unaware of.
  - Cross Site Scripting attacks usually come in the form of JavaScript however, any active content poses a potential danger.
- Prevention
  - Validate the users input against what is expected
  - Encode user supplied output
  - After you believe you've done the right things during code development, inspect your code with a scan.

OWASP Top 2: Injection Flaws (SQL Injection)

- What is SQL Injection
  - SQL injection is the actual injection of SQL commands into web applications through user input fields.
  - When an application uses internal SQL commands and you also have user input capabilities (like a login screen), SQL commands can be injected that can create, read, update, or delete any data available to the application.
- Prevention
  - You can put tight constraints on user inputs. But the best method of preventing SQL injection is to avoid the use of dynamically generated SQL in your code. Instead use stored or canned procedures.
  - And then again, run a scan to make sure your application is not vulnerable to SQL injections.

OWASP Top 3: Malicious File Execution

- What is Malicious File Execution
  - When Developers program applications to use input files provided by the user and the bad guy is the one entering the file, a malicious file is executed unknowingly, thus we have malicious file execution.
  - Malicious file execution attacks can occur anytime the application accepts filenames or files from a users.
  - When these files are executed, they can be used to do just about anything from stealing data to taking over the entire system.
- Prevention
  - Strongly validate user input using "accept known good" as a strategy, or isolate incoming files and check them legitimacy before executing them.
  - Disable certain PHP commands: I suggest that you visit the OWASP website to see what commands to disable.

Other Vulnerabilities

- Code Mistakes
- Untrained Users
- Insecure Configuration Settings

CYBER SECURITY – PRECAUTIONS

1. Install OS/Software Updates

2. Run Anti-virus Software

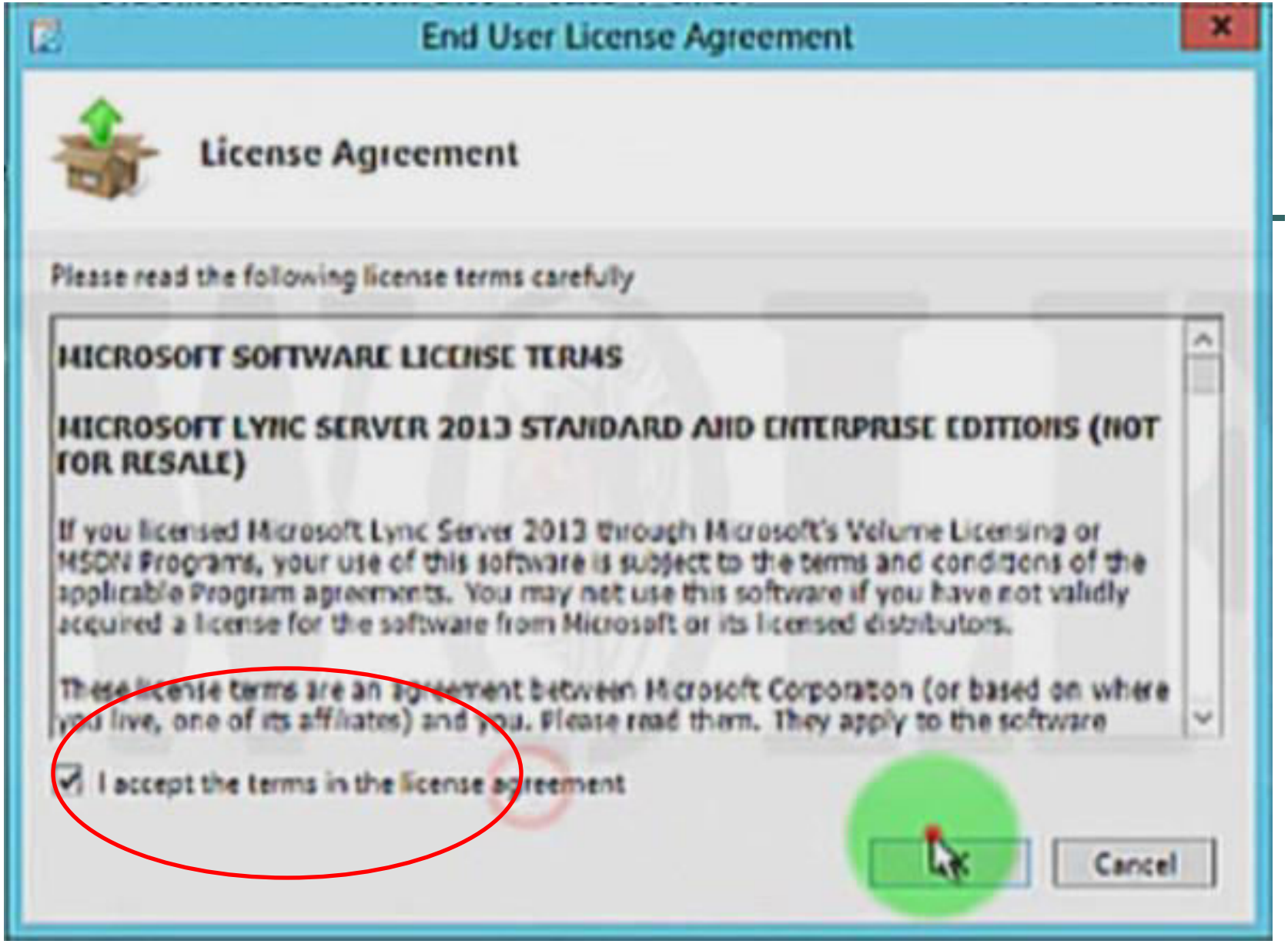
3. Prevent Identity Theft

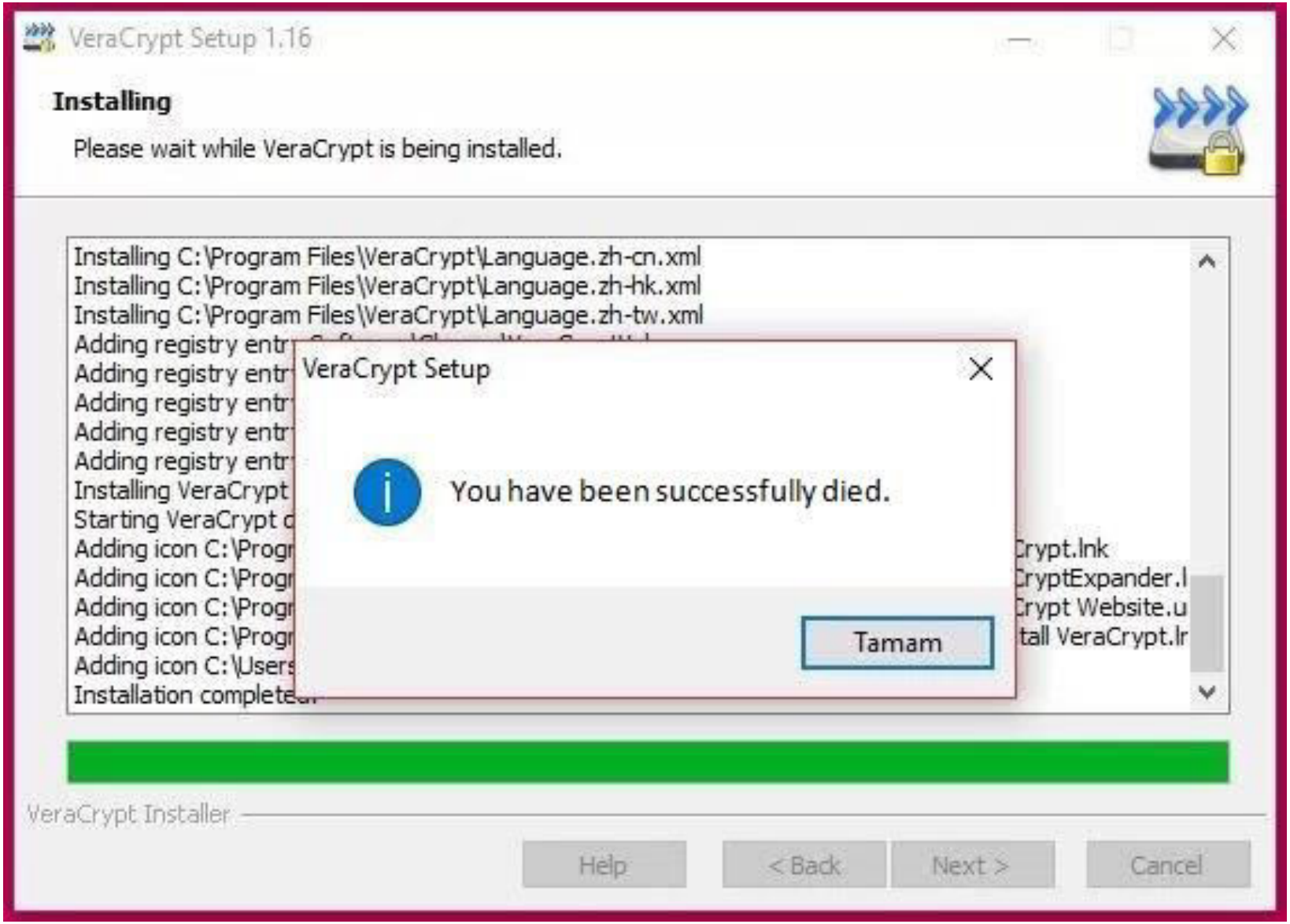
4. Turn on Personal Firewalls

5. Avoid Spyware/Adware

6. Protect Passwords

7. Back up Important Files


End User License Agreement
License Agreement
Please read the following license terms carefully
MICROSOFT SOFTWARE LICENSE TERMS
MICROSOFT LYNC SERVER 2013 STANDARD AND ENTERPRISE EDITIONS (NOT FOR RESALE)
If you licensed Microsoft Lync Server 2013 through Microsoft's Volume Licensing or MSDN Programs, your use of this software is subject to the terms and conditions of the applicable Program agreements. You may not use this software if you have not validly acquired a license for the software from Microsoft or its licensed distributors.
I accept the terms in the license agreement
Cancel


VeraCrypt Setup 1.16
Installing
Please wait while VeraCrypt is being installed.
Installing C:\Program Files\VeraCrypt\Language.zh-cn.xml
Installing C:\Program Files\VeraCrypt\Language.zh-hk.xml
Installing C:\Program Files\VeraCrypt\Language.zh-tw.xml
Adding registry entr
Adding registry entr
Adding registry entr
Adding registry entr
Adding registry entr
Installing VeraCrypt
Starting VeraCrypt d
Adding icon C:\Progr
Adding icon C:\Progr
Adding icon C:\Progr
Adding icon C:\Progr
Adding icon C:\Users
Installation complete
Crypt.lnk
CryptExpander.l
Crypt Website.u
tall VeraCrypt.lr
VeraCrypt Setup
You have been successfully died.
Tamam
VeraCrypt Installer
Help
< Back
Next >
Cancel

Keylogger

- What's a Keylogger and how does it exploit a Web Application?
  - Downloaded unknowingly
  - Resident on Personal Computers
  - Captures User Activity
  - Usually part of a malicious Network or BOTNET

Keylogger Mitigations

- Train users
- Implement effective Anti-Spyware, Anti-Virus
- Keep patches and versions current
- Firewall
- Automatic form filler programs
- Cut and paste
- One-time passwords
- Smartcards
- Virtual keyboards

How Much Security is Enough?

- Security based on Cost vs. Risk

Threat * Vulnerability = Risk

Cost of Implementing Controls – Cost of not Implementing Controls = Cost

Cyber Security – Social Engineering Attack

Social engineering is the art of manipulating people so they give up confidential information. The types of information these criminals are seeking can vary, but when individuals are targeted the criminals are usually trying to trick you into giving them your passwords or bank information,

So•cial En•gin•eer•ing

TYPES OF ATTACKS

PHISHING	SPEAR PHISHING	VISHING
		
SMISHING	**MINING SOCIAL MEDIA**	**LEARN MORE**
		 www.vasco.com/crontosign


SOCIAL
ENGINEERING
Psychological
Manipulation
Phishing
Pretexting
Baiting

What is Social Media?

Social Media refers to forms of electronic communications through which users create online communities to share information, ideas, personal messages, and other contact.

To put it simply, it allows for the creation and exchange of user-generated content.

The Screen Challenge

Take a moment to total how much time you spend daily looking at a screen.

Then,

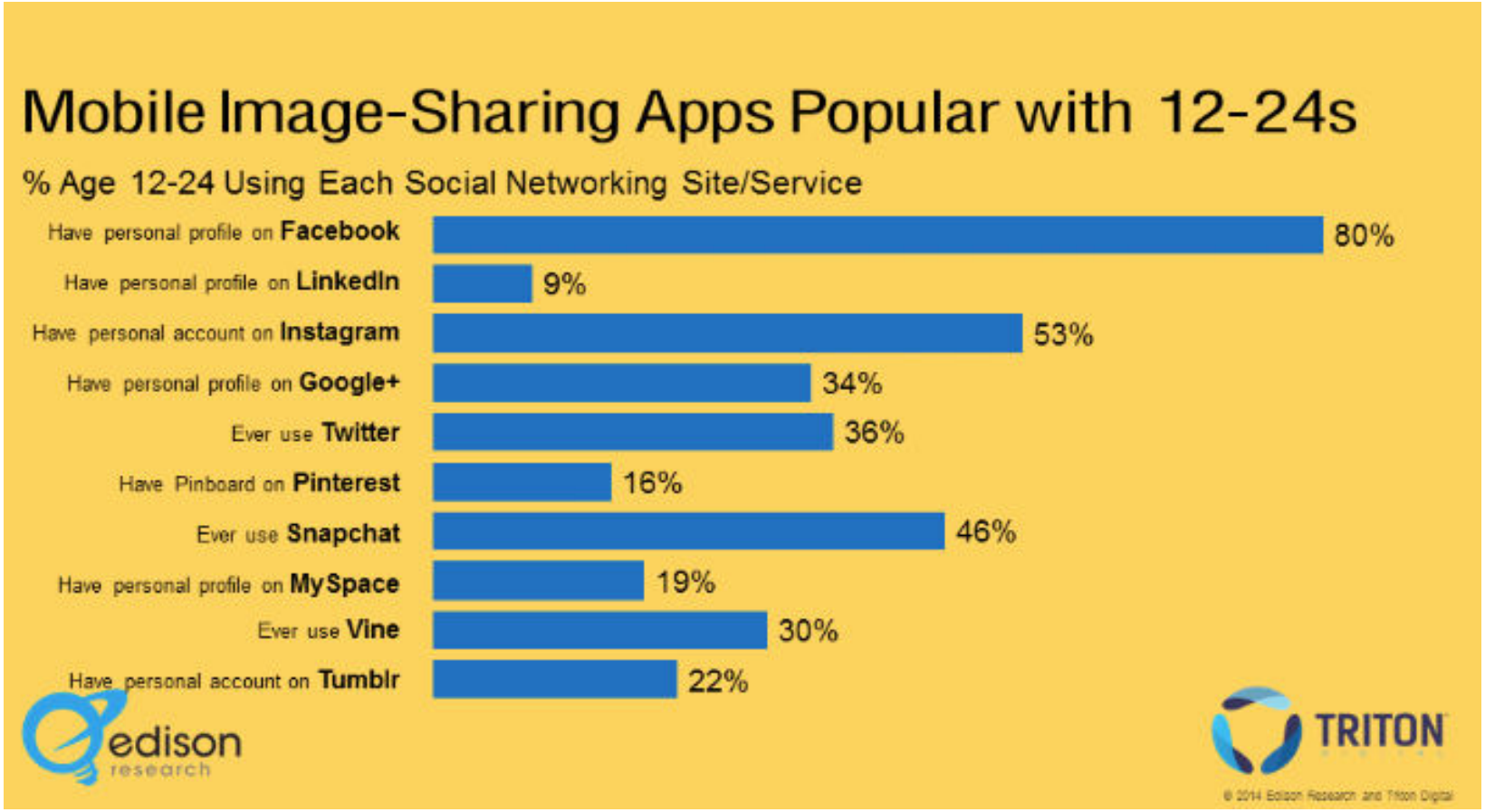
Take some time to estimate how much time your teenager spends looking at a screen.

Kids Today…

- 78% of teens have cell phones, almost half own smartphones
- 1 in 4 are “cell-mostly” internet users
- 23% of teens have a tablet
- 81% use social networking sites
- 8-18 year olds devote an average of 7 hours and 38 minutes to using entertainment media across a typical day
- 100% of EHS students have a laptop and access to the internet

POP Quiz!

What Social Media Are They Using?



What are they posting?

Personal info posted to social media profiles: Gender and age

% of teen social media users within each group who say they post the following to their social media profiles ...

	Teen Social Media Users	Boys (a)	Girls (b)	Teens 12-13 (a)	Teens 14-17 (b)
Your real name	92%	92%	92%	89%	93%
A photo of yourself	91	89	94	82	94[a]
Your interests, such as movies, music, or books you like	84	84	85	81	85
Your birthdate	82	81	83	79	83
Your school name	71	73	69	56	76[a]
The city or town where you live	71	73	69	67	72
Your relationship status	62	62	61	50	66[a]
Your email address	53	57	49	53	53
Videos of you	24	27	21	25	24
Your cell phone number	20	26[b]	14	11	23[a]

Source: Pew Internet Teens and Privacy Management Survey, July 26-September 30, 2012. n=802 parents of teens ages 12-17 and 802 teens ages 12-17. The margin of error for teen social media users is +/- 5.1 percentage points.

Why Social Media Can't Be Ignored

	Registered Users	Active Users
Facebook	1+ billion	1 billion
Youtube	800 million	4 billion views per day
Skype	663+ million	280 million
Google+	500+ million	235 million
Twitter	500+ million	200+ million
Linkedin	200+ million	160 million
Dropbox	100+ million	100 million
Instragram	100+ million	100 million
Pinterest	25 million	

- Wikipedia, 2013

Why Social Media Can't Be Ignored

- There is a decline of print media
- Direct connection to your 'clients'
- Is become more and more widely accessible
- It's FREE!

23% of children between ages 0 and 5 use the Internet & 82% use it on a weekly basis

650+million active users on Facebook

1 billion tweets are posted per week

#1 online activity beating porn & personal email for total time spent online

50% log in per day

460k new accounts are created on Twitter per day

YouTube has **490+million** users worldwide

---

92 billion page views each month

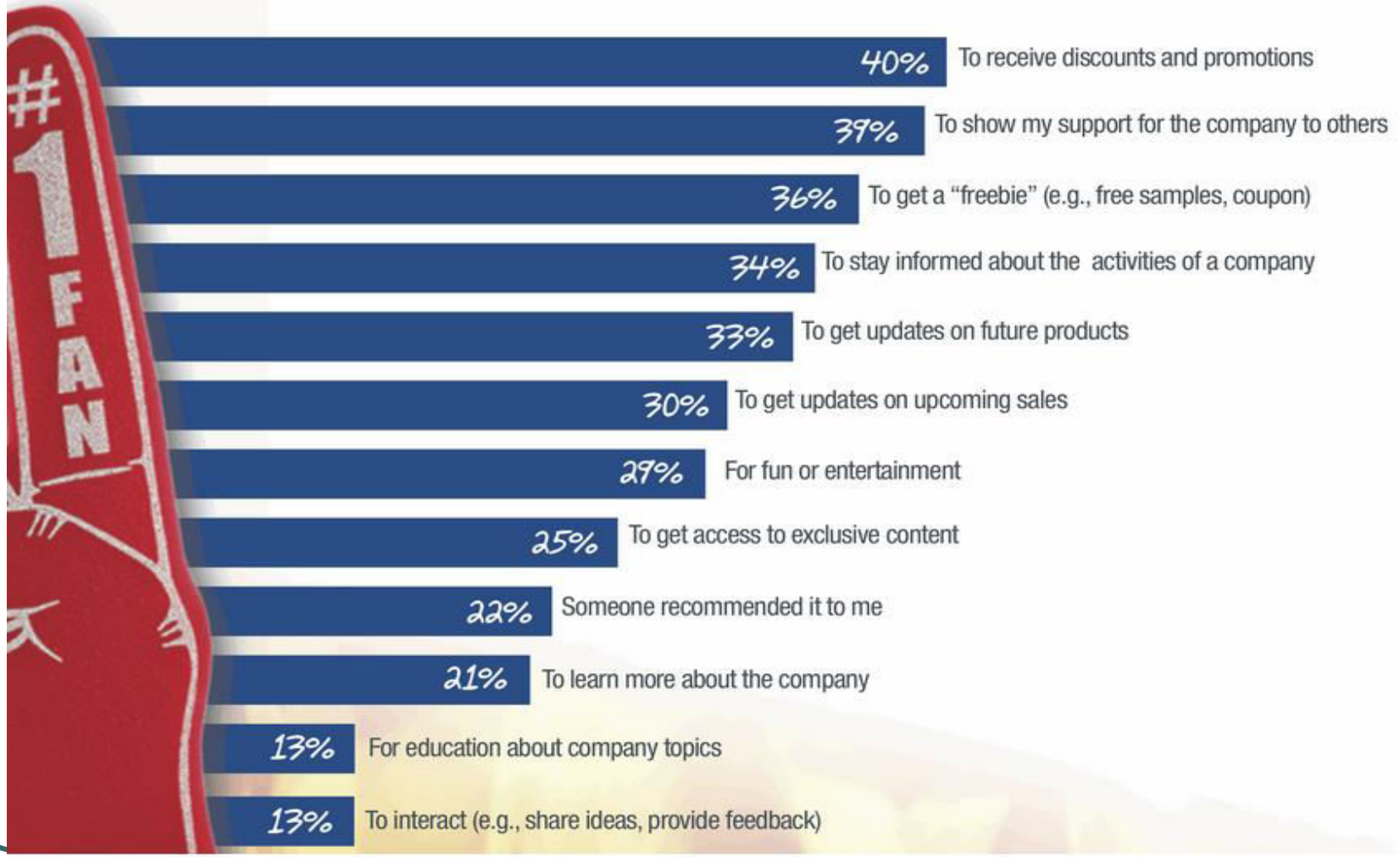
400 tweets per minute containing a YouTube link

More video content is uploaded to YouTube in a 60 day period than the three major U.S. television networks created in 60 years.

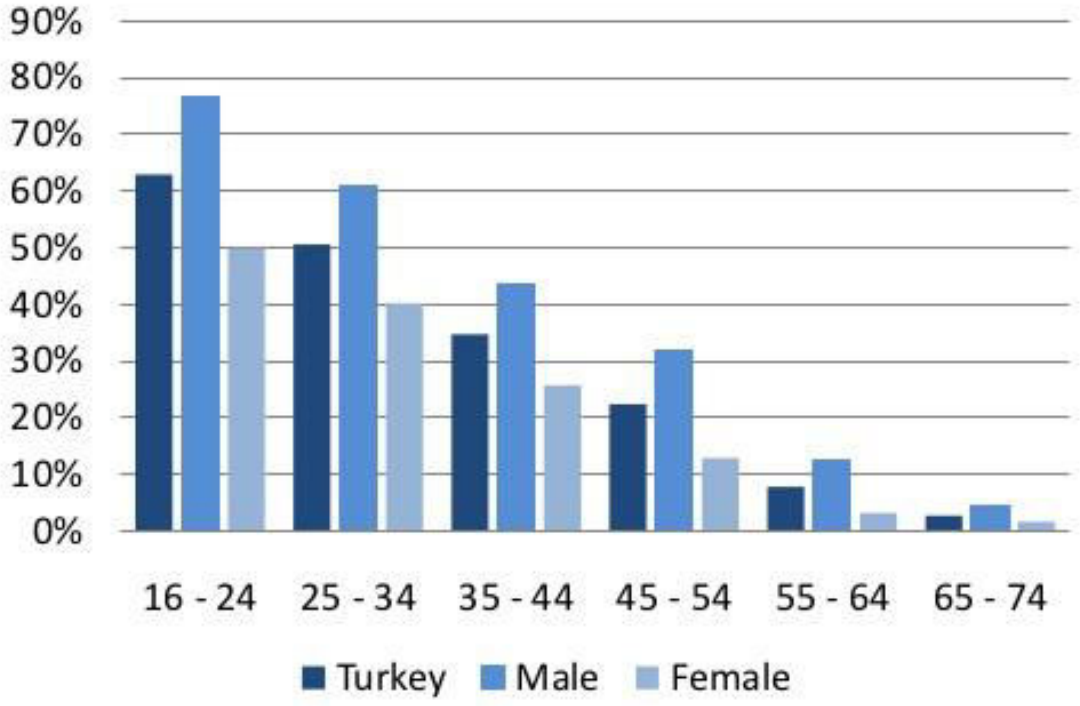
78 million monthly visitors on Wikipedia

90 million users on LinkedIn

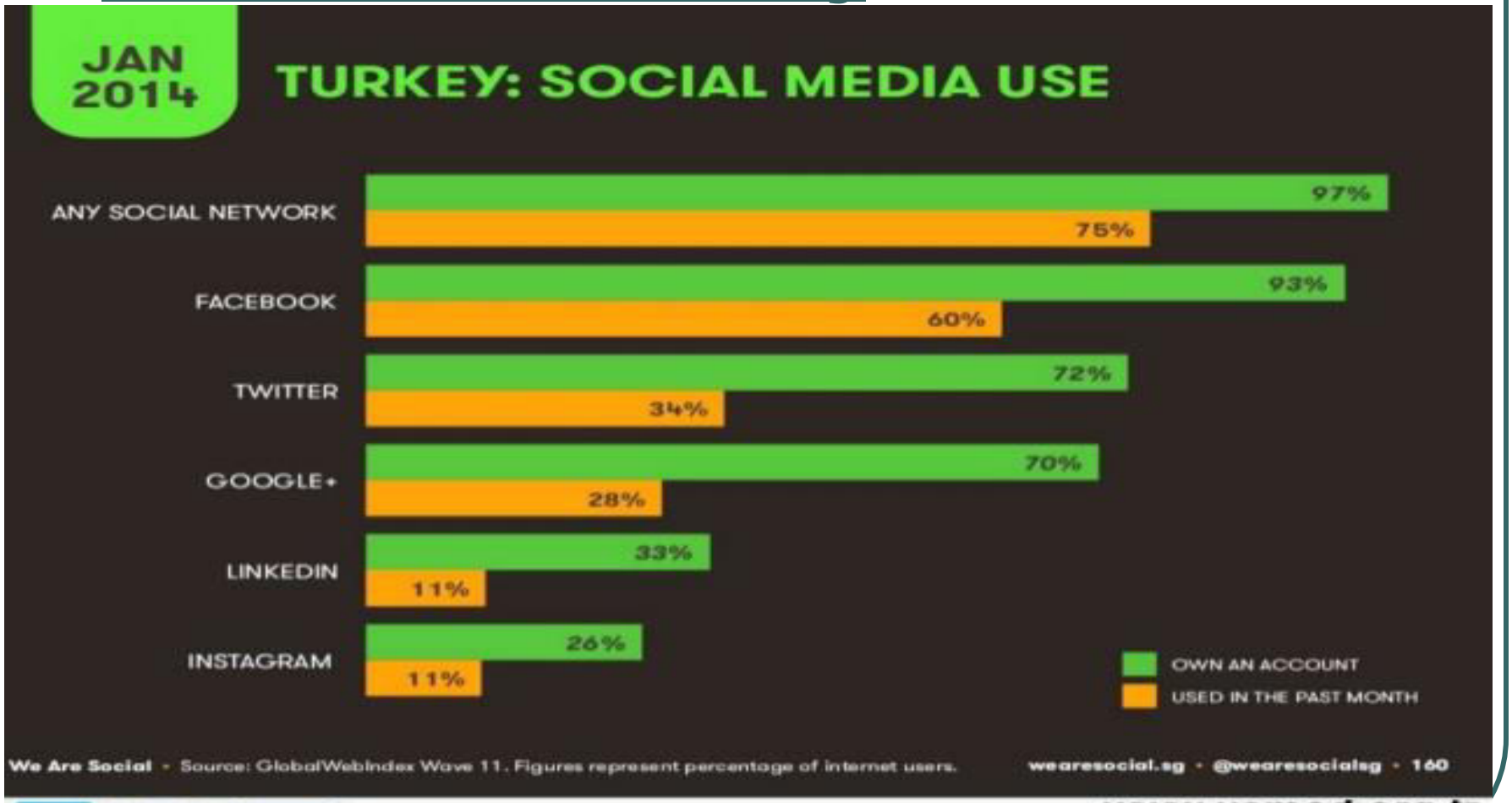
WHAT HAS MOTIVATED YOU TO "LIKE" A COMPANY, BRAND, OR ASSOCIATION ON FACEBOOK?



Internet usage by age groups



Social Media - Turkey



USMED Uluslararası Sosyal Medya Derneği

www.usmed.org.tr
twitter.com/saidercan

"Social Media Marketing: Enables Others to Advocate for Your Business Through Compelling Content"

Image credit: Ian Sane

Social Media is Like a Cocktail Part
Listen Then Respond”

Photo Credit:
The Dana


“Links are the Currency of the Social Web”

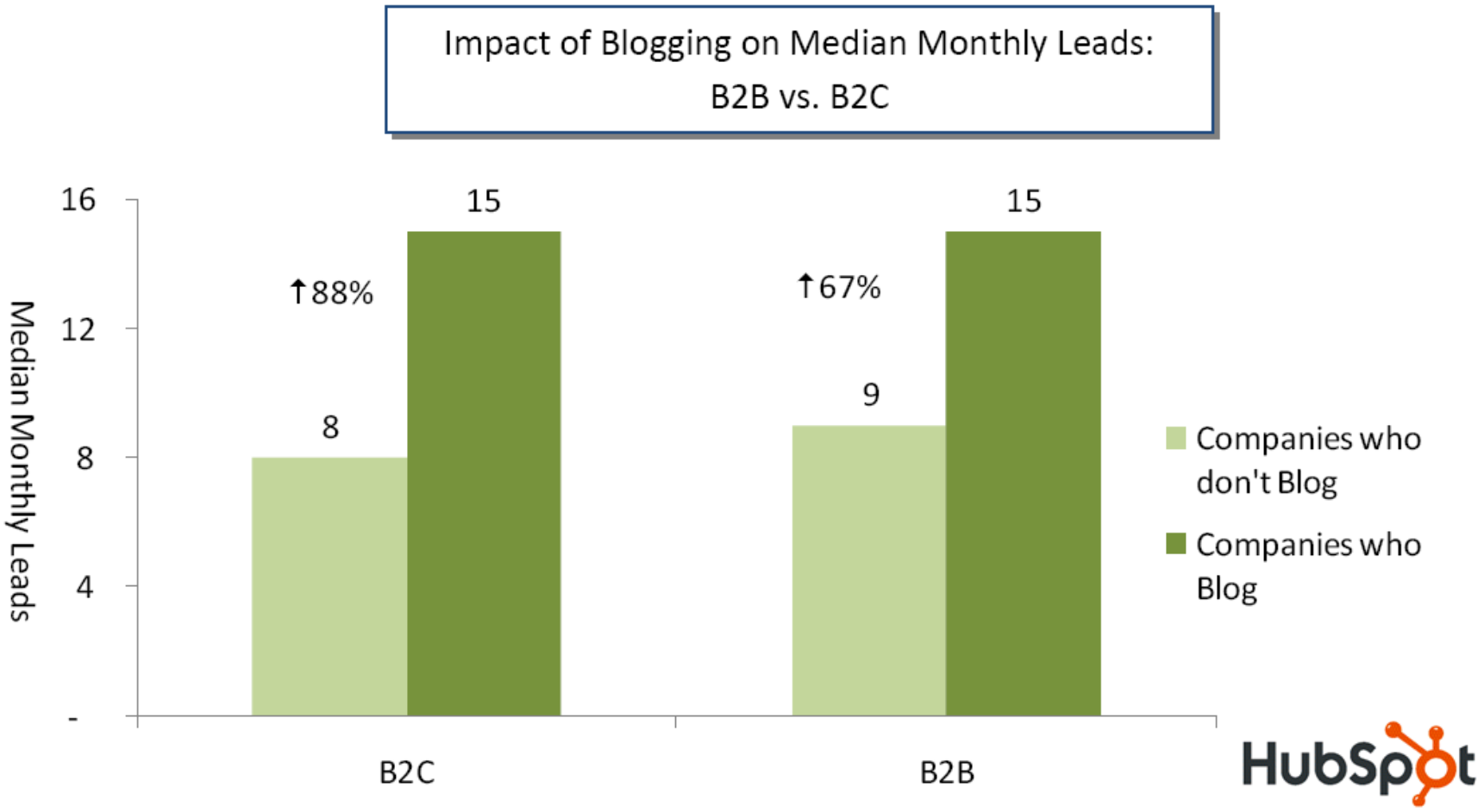
"Facebook is a social network that *connects* people personally and professionally through connections, messages, photos, & videos."

Photo Credit: Marvin Kuo

"Twitter is like a Text Message with a BCC: To The World"

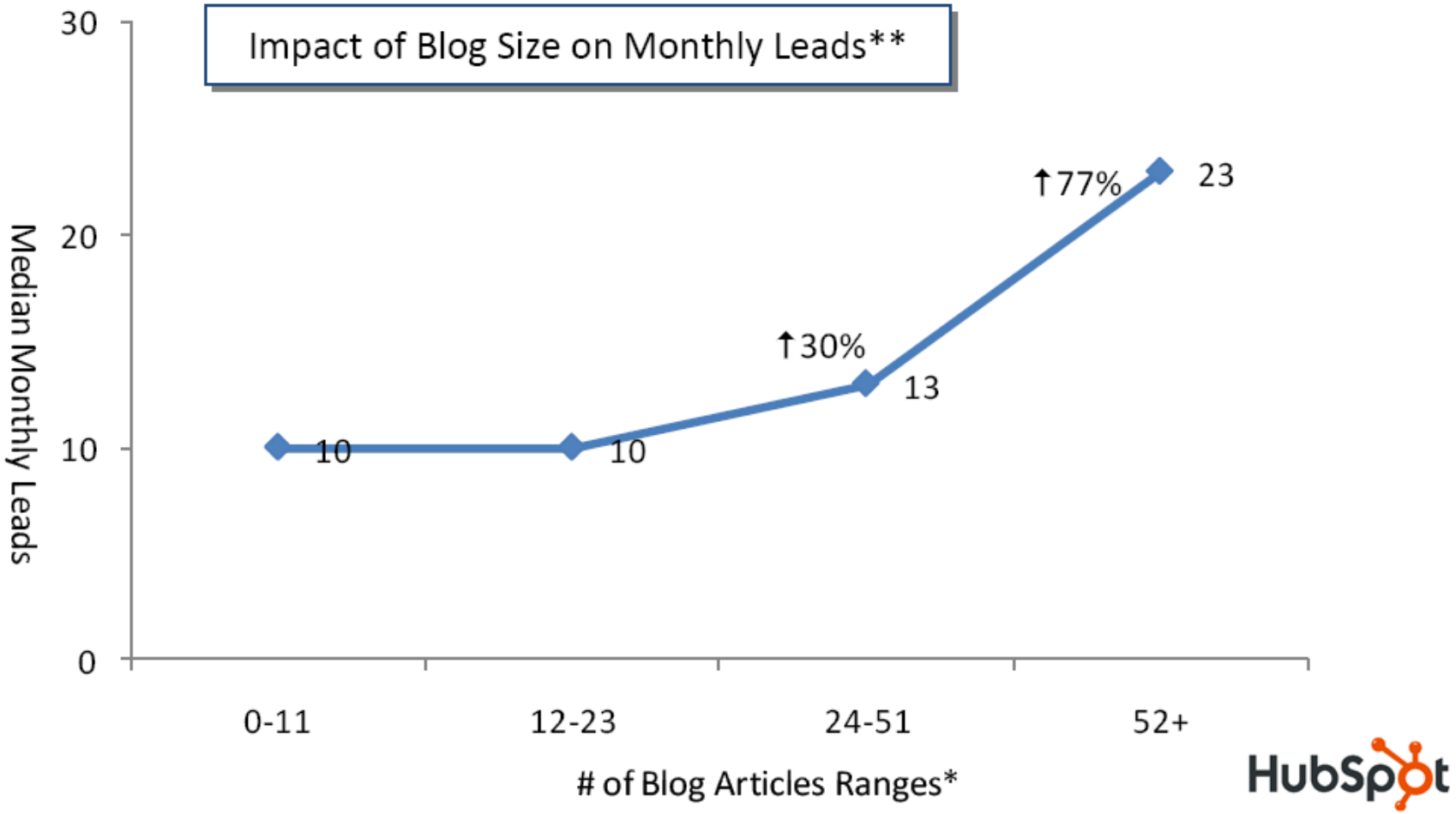
Photo Credit: ydhsu

Blogging and B2C and B2B Leads



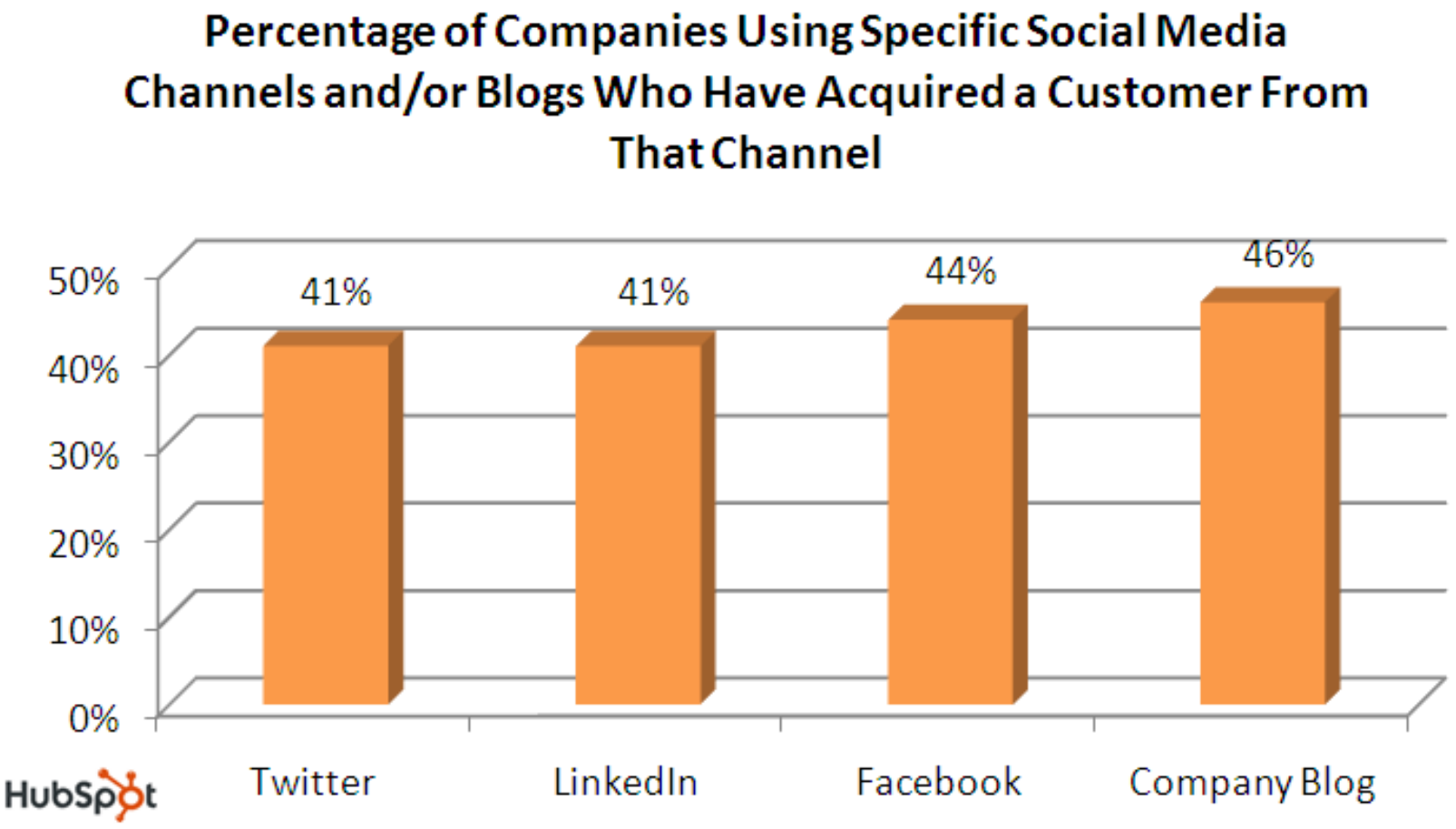
Source: State of Inbound Marketing Lead Generation Report - http://bit.ly/cVMpkn

Blog Articles By Leads Generated



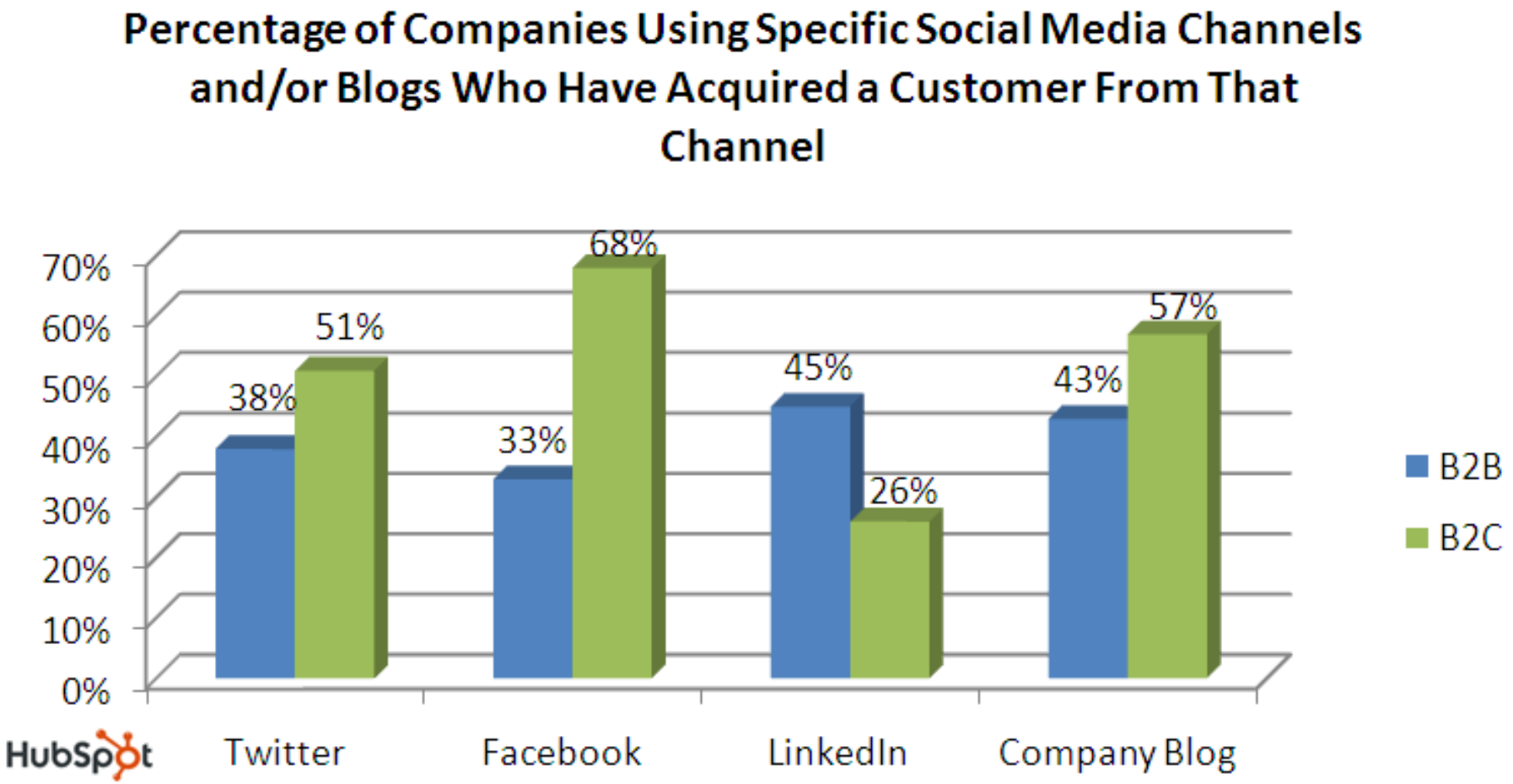
Source: State of Inbound Marketing Lead Generation Report - http://bit.ly/cVMpkn

Social Media is for Leads and Sales



Source: State of Inbound Marketing Report - http://bit.ly/aewfHr

Social Media is for B2B and B2C



Source: State of Inbound Marketing Report - http://bit.ly/aewfHr

Google – Power Usage

- 260 million watts – (1.1% to 1.5% of global electricity)
- Google Uses About 900,000 Servers
- 6 billion hours of video (2015)
- Nuclear Power stations are used

Dangers of Social Media

What we know about teens:

- They are constantly trying to define themselves.
- They crave positive feedback to help them see how their identity fits into their world.
- They use social media for this feedback... but they are looking in a dangerous place.

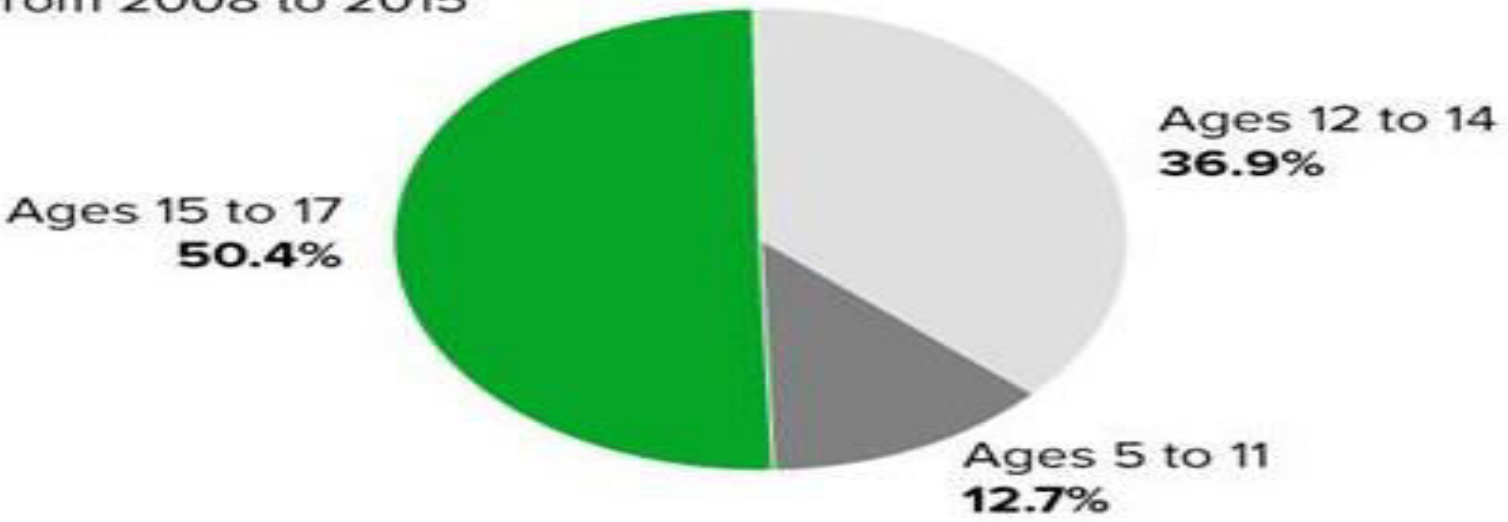
How is this harmful:

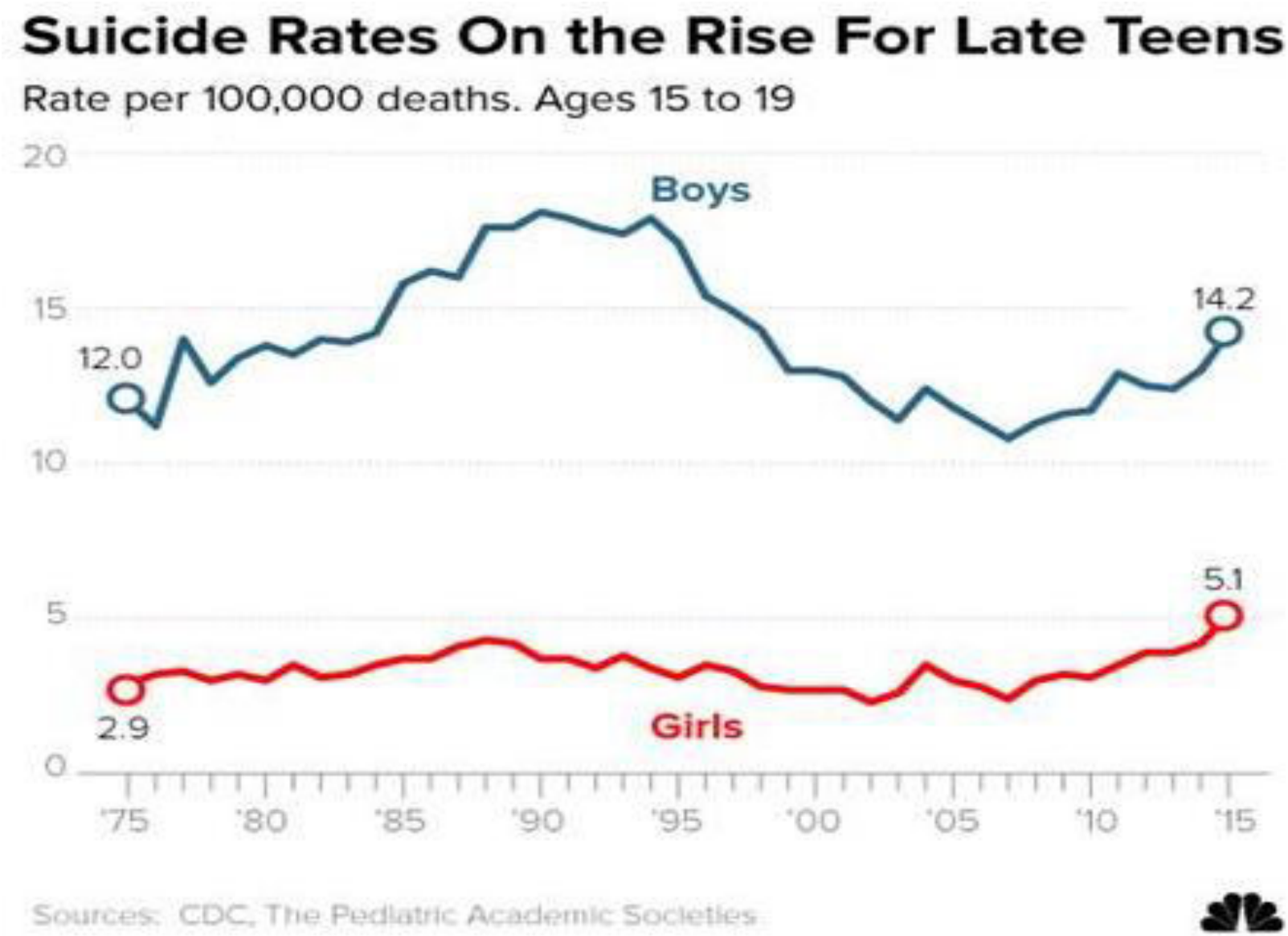
- The danger exists in the possibility of a very public rejection because negative feedback is there for anyone and everyone to see.
- Another danger is that teens ask for feedback without learning first that not everyone will respond in a supportive way.

Suicide-Related Hospital Admissions Nearly Double For Children

And More Than Half Of The Patients Were Late Teens

From 2008 to 2015




Suicide Rates On the Rise For Late Teens
Rate per 100,000 deaths. Ages 15 to 19
20
15
10
5
0
Boys
12.0
14.2
5.1
2.9
Girls
'75
'80
'85
'90
'95
'00
'05
'10
'15
Sources: CDC, The Pediatric Academic Societies

Blue Whale online suicide game

Turkey Suicide Hotlines

182

Cyber Security – Email Attack

Fake Email:

Sites:

- https://emkei.cz/
- www.anonymailer.net/
- http://www.sendanonymousemail.net/
- http://deadfake.com/Send.aspx

Fake Email – How to Identify

https://mxtoolbox.com/EmailHeaders.aspx

```
Return-Path: <xxxxx@gmail.com>
Received: from  (bf240.xxx.xxxx.com. [61.197.23.240])
        by mx.google.com with ESMTPS id pb4sm20464671pbc.55.2012.05.13.17.56.12
        (version=SSLv3 cipher=OTHER);
        Sun, 13 May 2012 17:56:13 -0700 (PDT)
Message-ID: <4fc05e2d.e4a9440a.302b.ffffe399@mx.google.com>
Date: Mon, 14 May 2012 00:56:10 +0900
From: xxxxx@gmail.com
Subject: Test
Content-Transfer-Encoding: Quoted-Printable
Content-Disposition: inline
Mime-Version: 1.0
Reply-To: xxxxx@hotmail.com
X-Priority: 3
To: yyyyy@gmail.com
Content-Type: text/plain; charset="iso-8859-1"
```

```
=E4=C4=F6=D6=FC=DC=DF


.
```

Cyberspace – Unclosed Eye

- *Wake up by 6.00 am*
- *Started from Home – 7.00 am, Besiktas*
- *Used Metro Bus till zeytinburnu*
- *Used Metro rails till YTU, Davutpasa*
- *Had food at 8.30 am, Which food ?, How much ?*
- *Smoked four time*
- *Fought with friend*
- *Low Money in the bank account*
- *Had taken mecicine*
- *Shopped Fruits and Napkins*
- *Etc.,*

Mobile Security in Cyber Space

- *A Paid Spy !*
- *24 X 7 with you !*
- *Wherever you go, he follows you*
- *Have you checked the App permission ?*

Discussion / Suggestions ?

tsmuthu@hindustanuniv.ac.in