Computer & Network Security

- Computer security….why the need?
- CIA
- Authentication & Authorization
- Standalone Computer
- Passwords
- Smartcards
- Biometric Data
- Data Destruction
- Social Engineering
- Zombie computer
- Cybercrime
- Hackers & Crackers
- Malware (virus, Trojan horse, worm, rabbit)
- Ransom-Ware
- Spyware
- Antivirus software
- Denial of Service (DoS) attack
- Packet sniffing
- Security Policy

Computer/Network Security…….Why?

Online banking
Online stores or websites
Viruses damage computer files or the computer itself
Steal or edit personal information

Major technical areas of computer security are usually represented by the initials **CIA:**

- **C**onfidentiality
- **I**ntegrity
- **A**uthentication
- **A**vailability

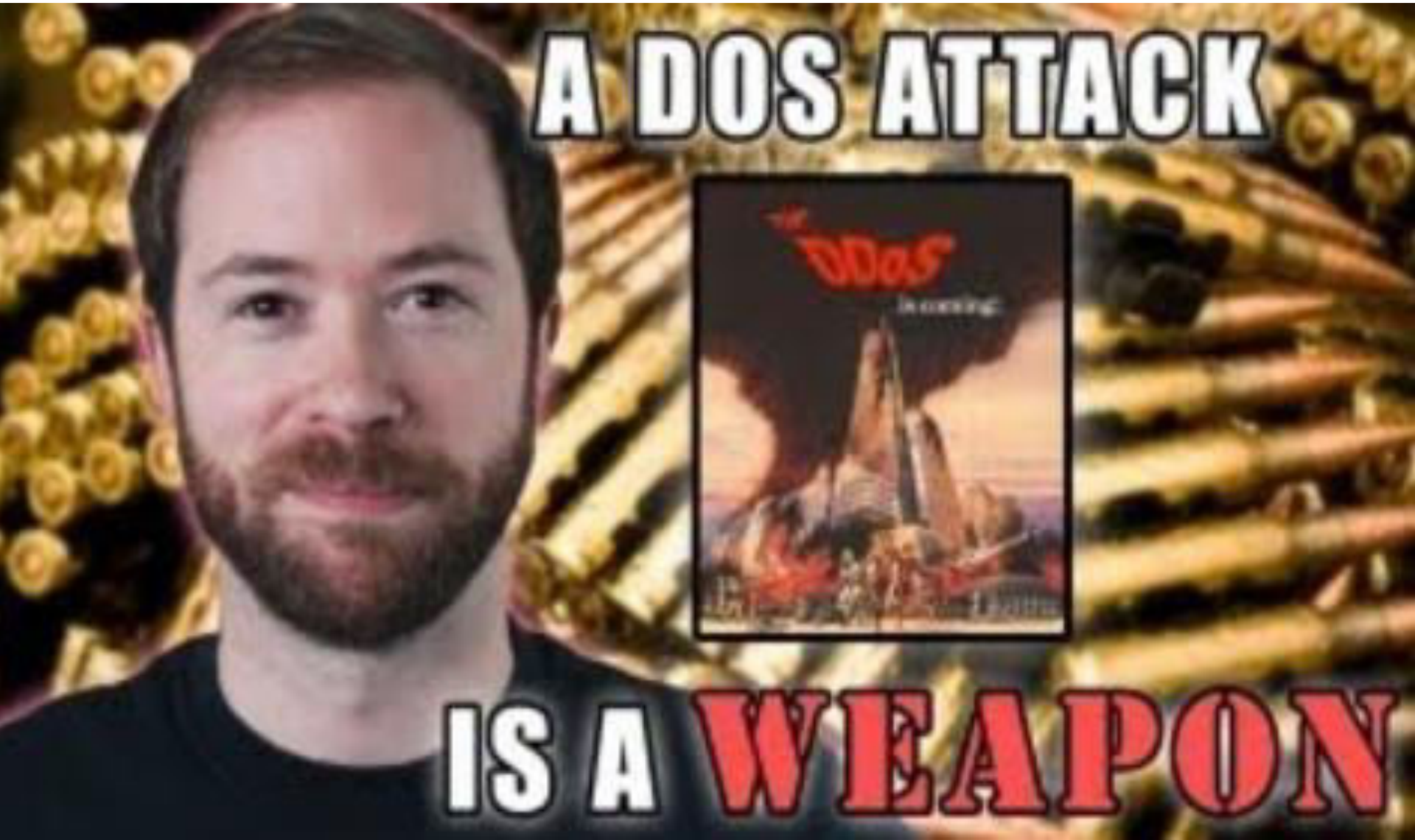
Confidentiality or Secrecy or Privacy: information cannot be accessed by unauthorized parties

Integrity

Information is protected against unauthorized changes that are not detectable to authorized users.

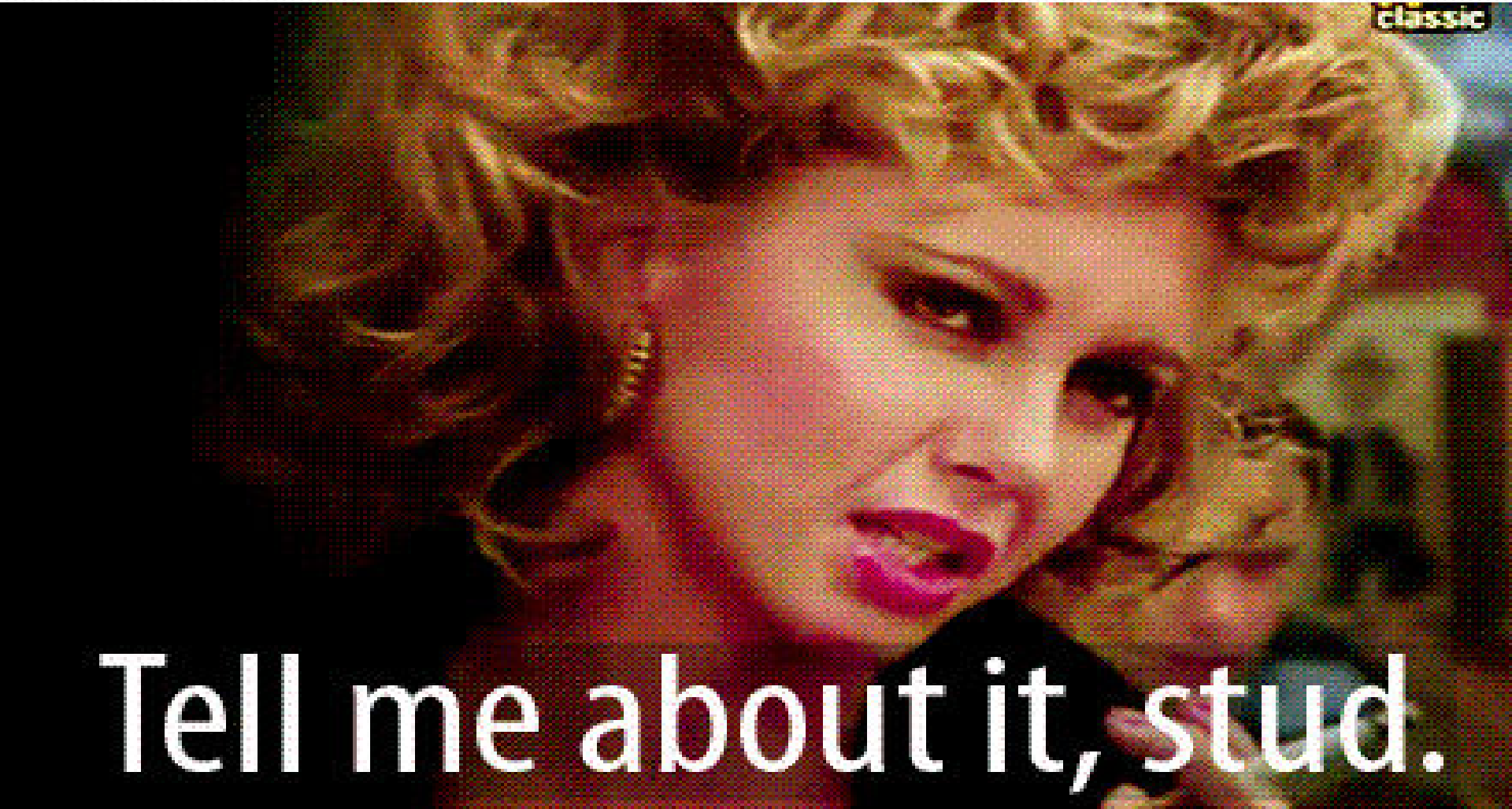
Authentication: users are who they claim to be

Availability: resources are accessible by authorized parties e.g. DOS attack



Other important concerns for computer security professionals

Access Control and **Non-repudiation**



Maintaining **access control** means not only that users can access only those resources and services to which they are entitled

but

also that they are not denied resources that they legitimately can expect to access.

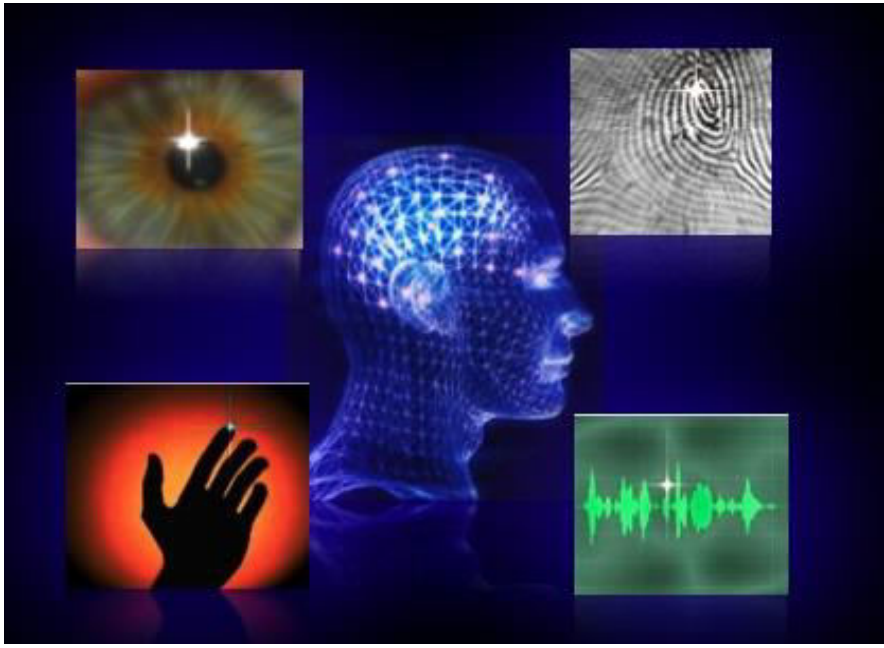
Non-repudiation implies that a person who sends a message cannot deny that he sent it and

conversely

A person who has received a message cannot deny that he received it.

Authentication

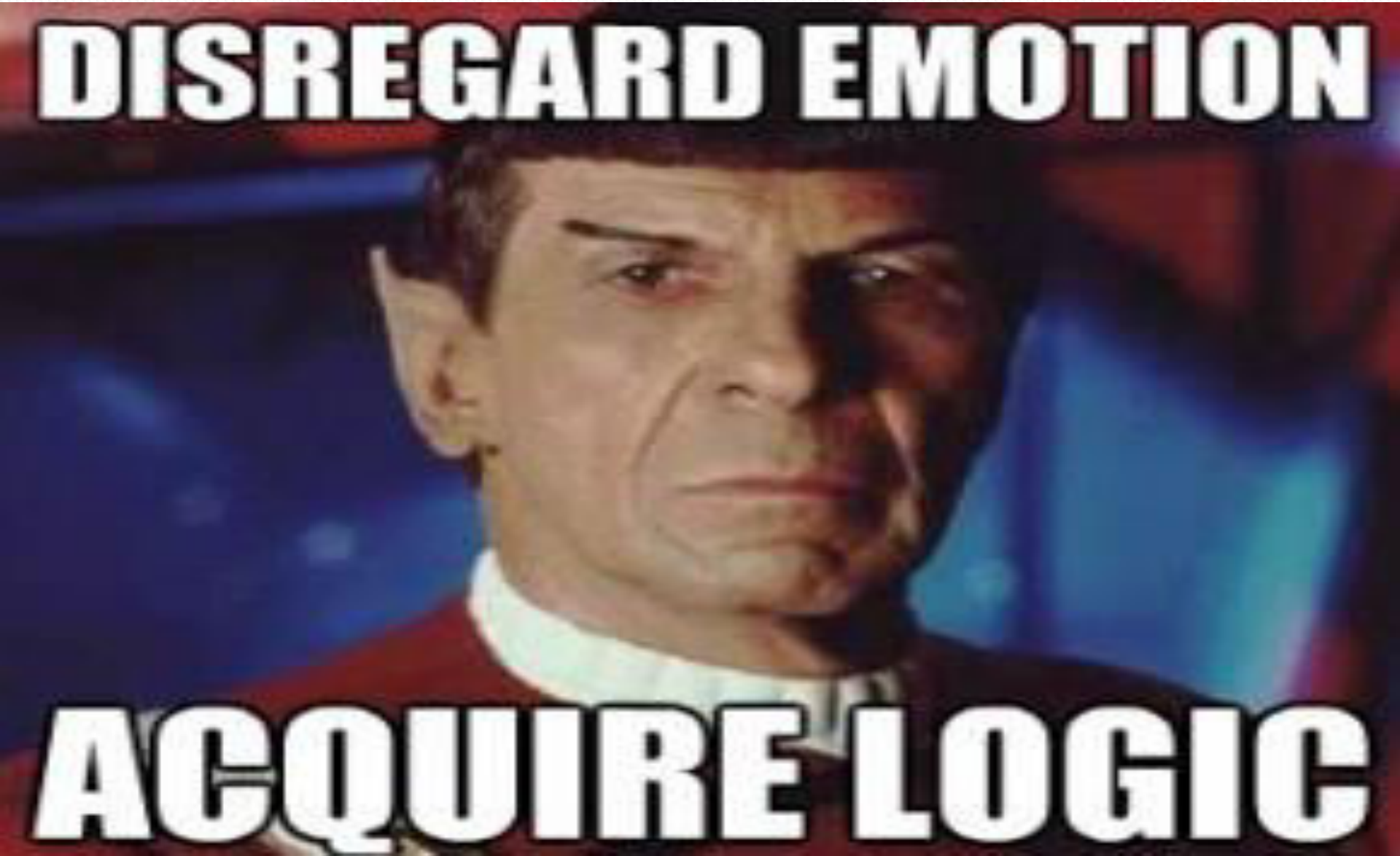
- Verifies a users identity i.e. usually based on username & password
- Ensures that the individual is who he or she claims to be
- Says nothing about the access rights of the individual



Authorization

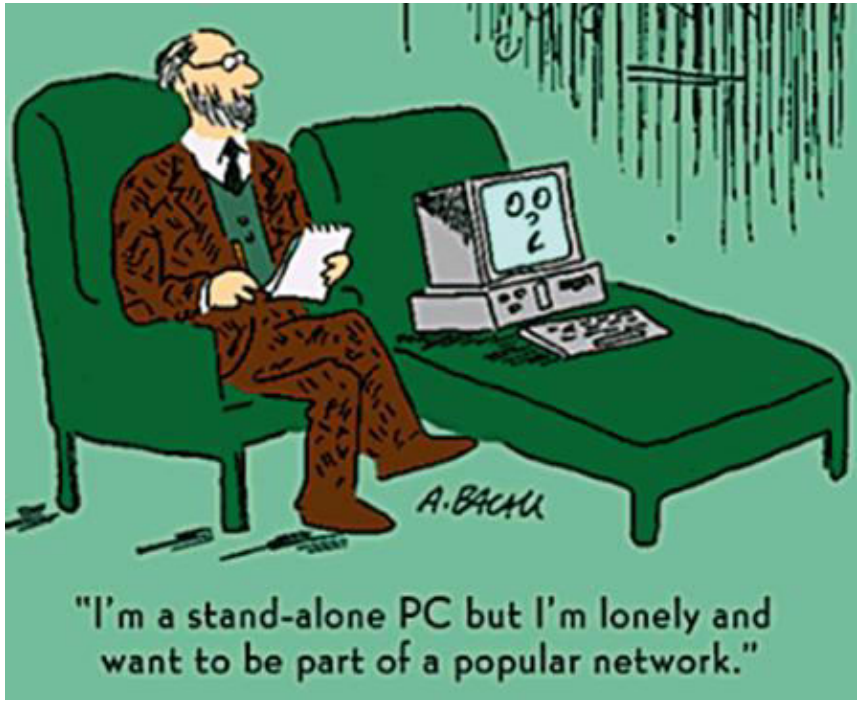
- Determines whether an authenticated person is allowed access to a service/resource e.g. access to which file directories
- In multi-user computer systems, a system administrator does the job

Logically, authentication precedes authorization



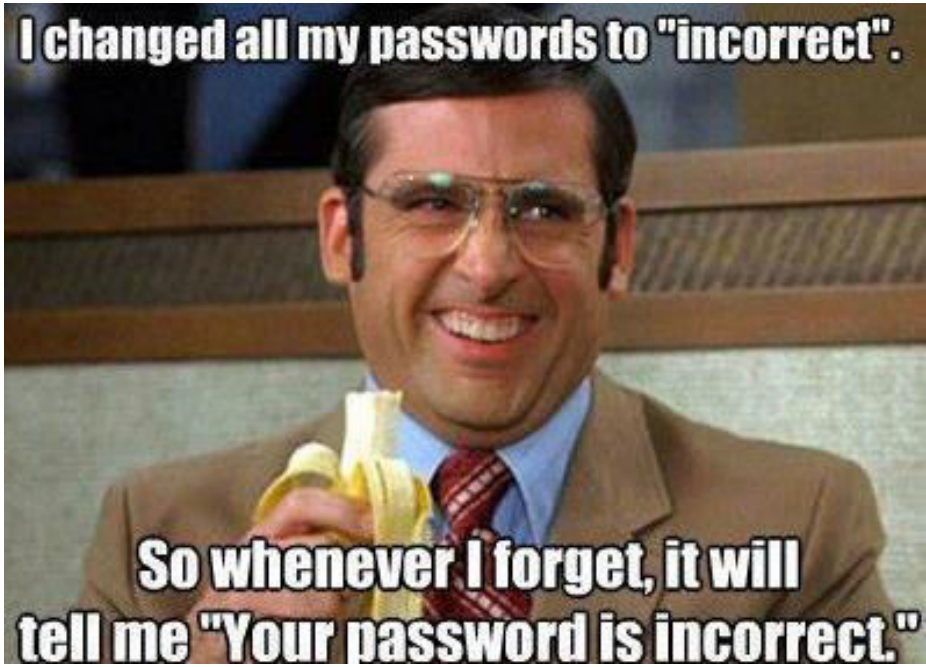
Standalone Computer

Computer that is not linked with the network i.e. no browsing the Web, no Facebook, no twitter or checking e-mail e



Content of a computer is vulnerable

Even if a standalone computer



Authentication Strategies

1. Something about the user is recognized as unique e.g. biometric, finger prints
2. Something the user possesses is unique (security token like a smart card)
3. Something the user knows (a password or PIN) is unique

Multi-factor or Two factor authentication……e.g., a bank card and a PIN

Passwords

- Essentially free
- Should be unique
- Should be unrelated to any of your other passwords.
- Shouldn’t write them down
- Shouldn’t you share them with anyone

Cracking Passwords

- **Theft**
- **Interception**: something that happens while the password is traveling through the computer, network, or the Internet i.e. only visit safe sites e.g. ***keyboard logger*** which is a malware program that runs on the computer, or a hardware device that has been inserted between the keyboard and the computer.
- **Guesswork….brute force**

Brute Force i.e. try every possible combination

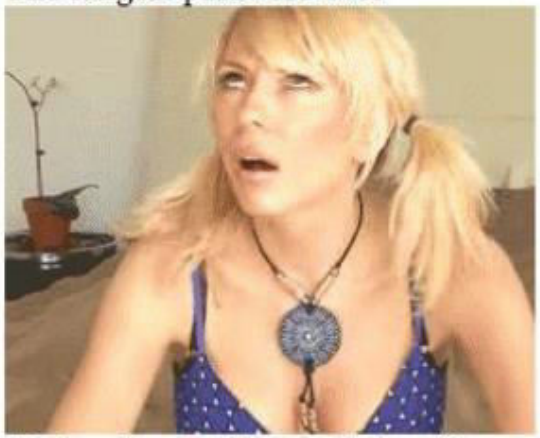
Bad Passwords

- Your name
- Names of family members or pets.
- Name of the street where you live.
- Your address.
- Your or family member's birthdate

Strong Passwords

- Relatively long.
- Complex
- Changed periodically.
- Never written down
- Do not use personal information
- Is not based on any dictionary word
- Watch for "shoulder Surfing"

The longest password ever



We laugh -- **but** her I. D. is safe.
During a recent password audit by a company, it was found that an employee was using the following password:
"MickeyMinniePlutoHueyLouieDeweyDonaldGoofySacramento"
When asked why she had such a long password, she rolled her eyes and said: "Hello! It has to be at least 8 characters and include at least one capital."

Steps that you can use to help you create passwords for your accounts

1. The **Strong** test: Is the password as strong (meaning length and content) as the rules allow?

2. The **Unique** test: Is the password unique and unrelated to any of your other passwords?

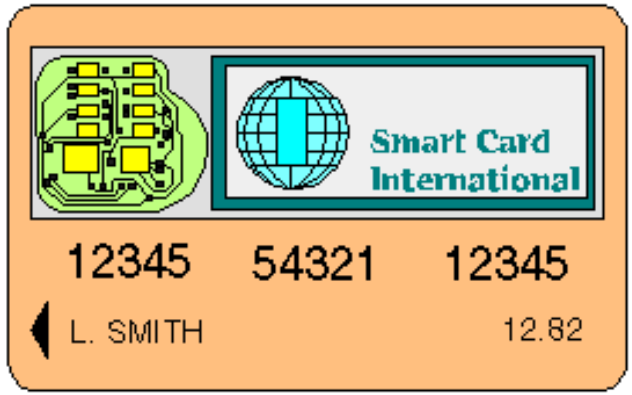
3. The **Practical** test: Can you remember it without having to write it down?

4. The **Recent** test: Have you changed it recently?

N.B. In spite of the **SUPR** tests, you need to be aware that sniffing happens

Smart Card

- Plastic card with embedded microprocessor chip, electronic memory, and a battery
- Of the several types of smart cards, some are **contact-less** (do not require to be swiped through a magnetic stripe reader) whereas others require **contact-with** the reader or the information may be **keyed in** by user
- When inserted into a reader, it transfers data to and from a central computer.



Variations of smart cards

Key fob

- Provide *two-factor authentication*: the user has a personal identification number, which authenticates them as the device's owner
- After the user correctly enters their PIN, the device displays a number which allows them to log on to the network

Wireless Token e.g. RFID badge

Memory Stripe Card

Biometric Data

Validates the person's physical body

Fingerprints, handprints, face, voice, retinal, iris, and handwritten signatures


Please lock the door
before leaving the room


Lock & Chain

Social Engineering

- Non-technical kind of intrusion that relies heavily on human interaction and often involves tricking other people to break normal security procedures.
- "**con game**" i.e. gain enough information from people to gain access to the network.

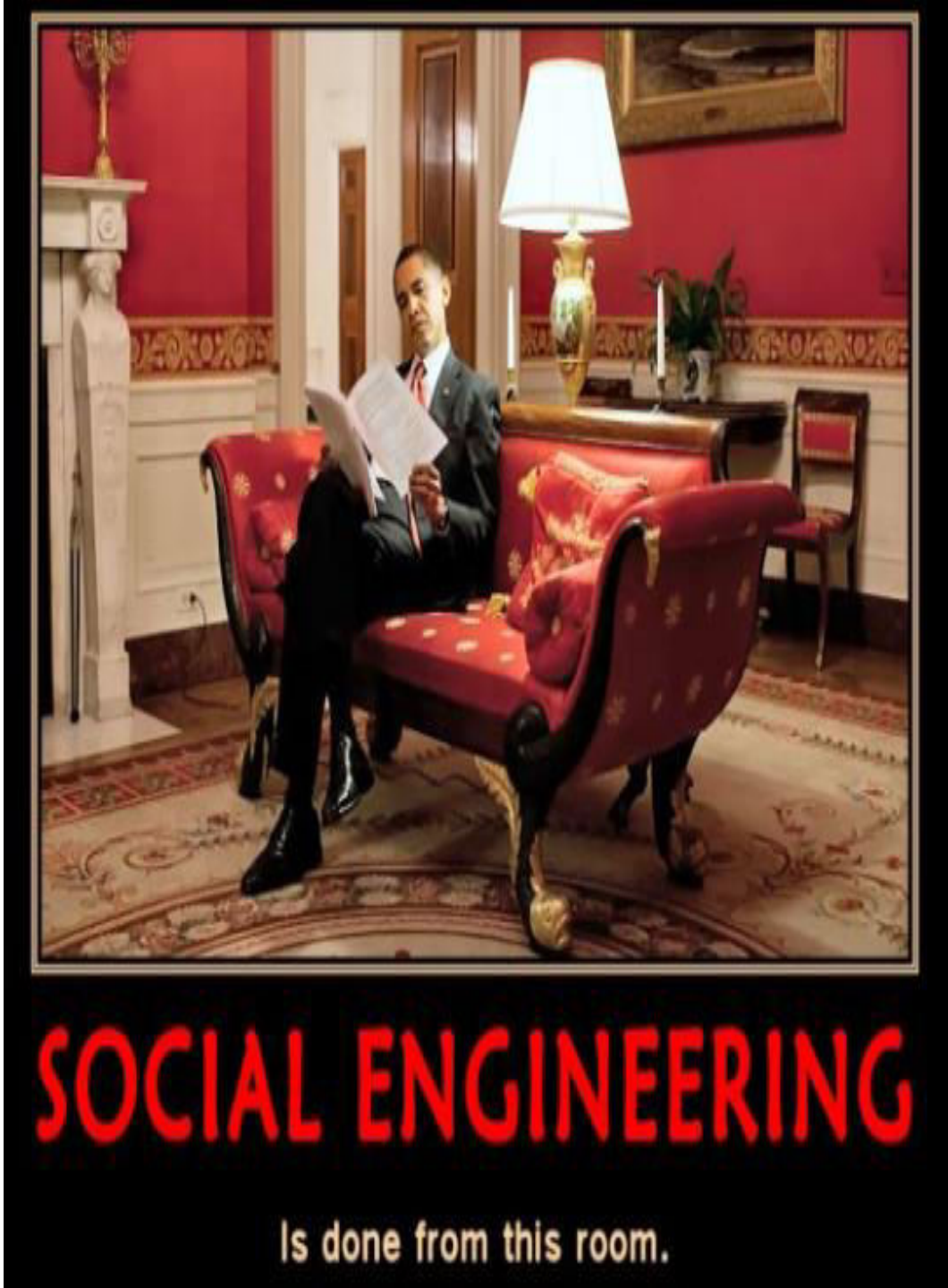
- Intruder would gain the confidence of someone who is authorized to access the network in order to get them to reveal information that compromises the network's security

- e.g. username and password (or they could go through your rubbish)

Social engineers often rely on the natural helpfulness of people

3 of the most commonly used social engineering techniques

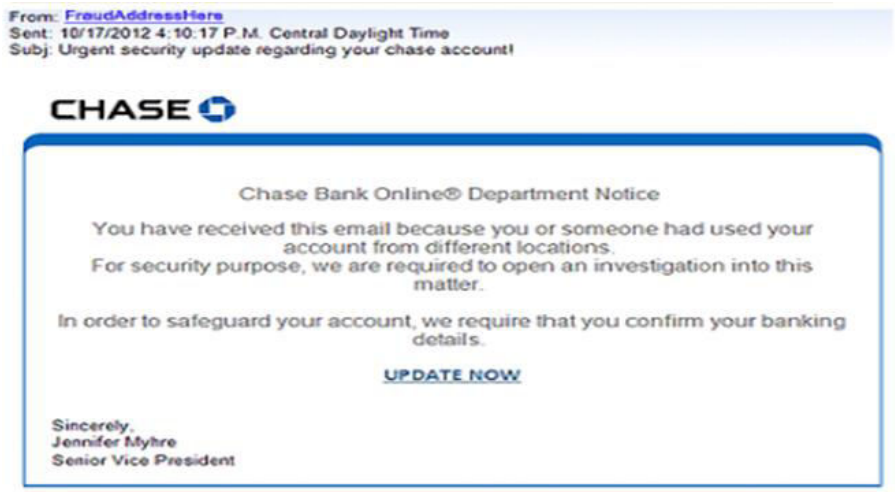
1. Pretexting
2. Phishing
3. Vishing



Phishing

Phishers send out e-mails that appear to come from legitimate websites

e.g. eBay, PayPal, or other banking institutions


From: FraudAddressHere
Sent: 10/17/2012 4:10:17 P.M. Central Daylight Time
Subj: Urgent security update regarding your chase account!

CHASE

Chase Bank Online® Department Notice

You have received this email because you or someone had used your account from different locations.
For security purpose, we are required to open an investigation into this matter.

In order to safeguard your account, we require that you confirm your banking details.

UPDATE NOW

Sincerely,
Jennifer Myhre
Senior Vice President

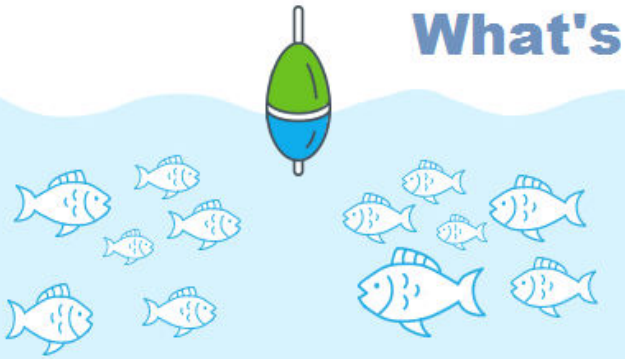
Pretexting

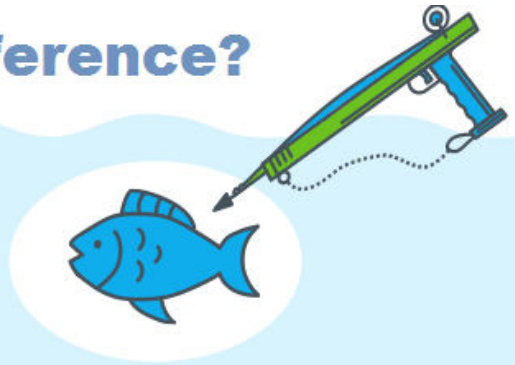
- Fraudulent acquisition of sensitive information usually over the phone.
- Attacker must be able to establish legitimacy with the intended target/victim.
- Requires some prior knowledge or research on the part of the attacker.

Vishing

- Automated calls or text messages to phones and cell phones with the specific goal of gaining personal information for the purposes of identity theft
- An unsuspecting user is sent a voice mail instructing them to call a number which appears to be a legitimate telephone-banking service.
- The call is then intercepted by a thief.

What's The Difference?





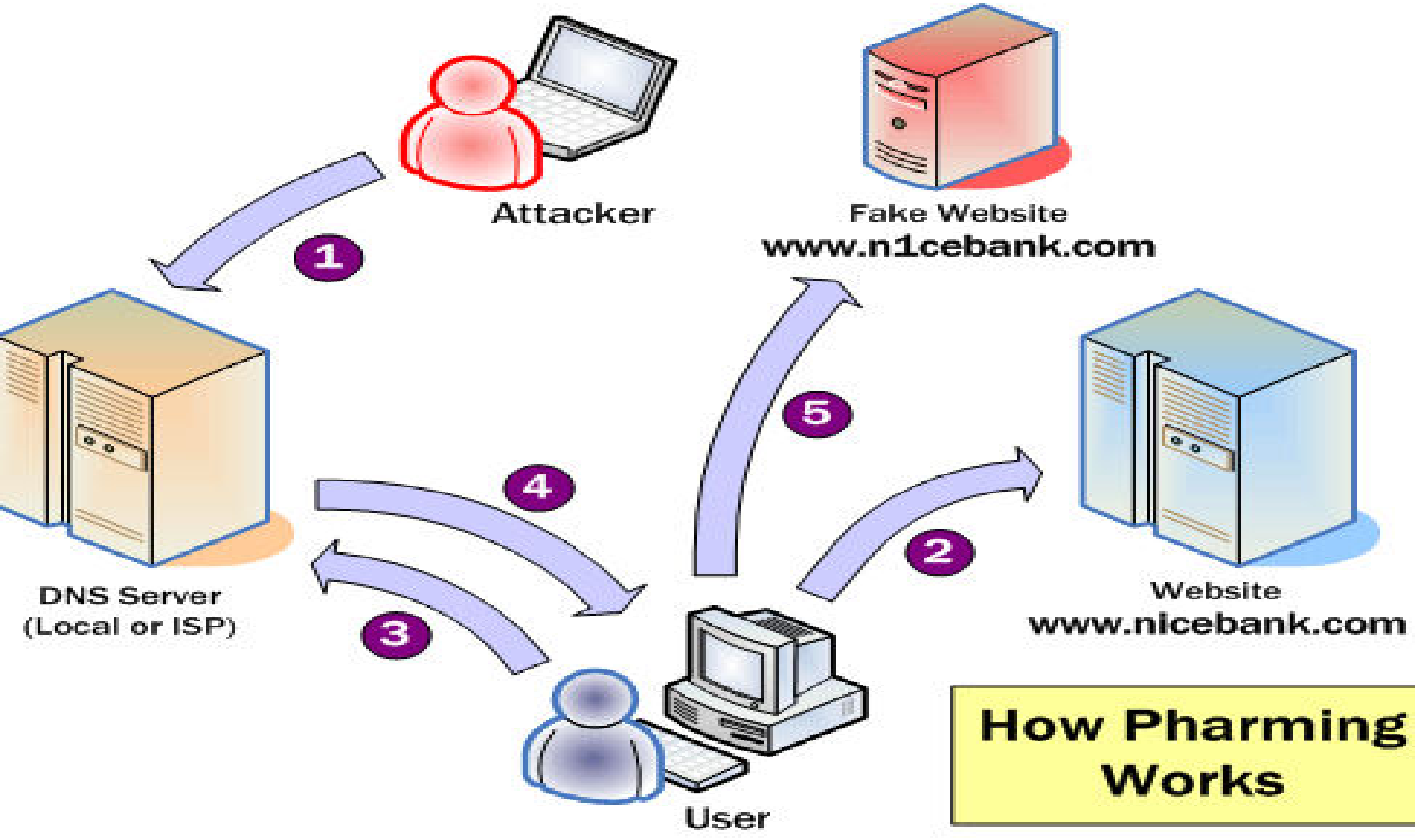
PHISHING

IS A BROAD, AUTOMATED ATTACK THAT IS LESS SOPHISTICATED.

SPEAR-PHISHING

IS A CUSTOMIZED ATTACK ON A SPECIFIC EMPLOYEE & COMPANY

Pharming: redirects users to false websites without them even knowing it



Solution

Educate users into NOT sharing information

on

How they access the network & Require identification from support staff.

Wardriving

- Specific kind of piggybacking.
- The broadcast range of a wireless access point can make internet connections possible outside your home, even as far away as your street.

Shoulder Surfing

- Bad guys don't even need a computer to steal your sensitive information
- By simply watching you, they can steal all kinds of sensitive, personal information.

Tailgating

- When someone who is unauthorized follows the employee through a secured entrance
- Also when someone continues to use a Windows session

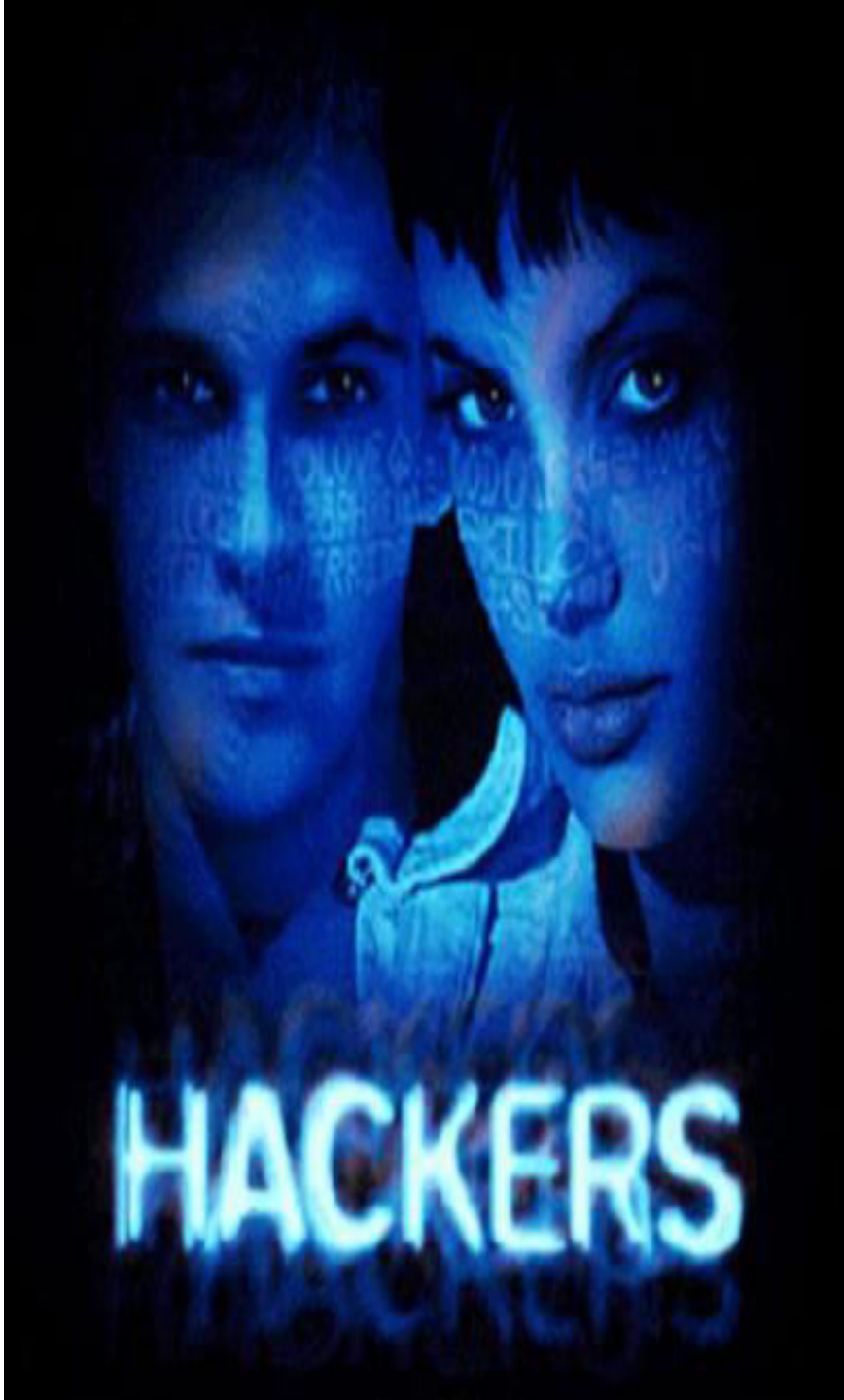
Give out passwords to anyone
Store passwords on a computer
Use same password on more than one system

Cybercrime

- Any illegal activity that uses a computer & Internet as its primary means of commission or for storage of evidence.
- e.g. downloading illegal music files, stealing millions of dollars from online bank accounts and the dissemination of computer viruses,

Someone who can gain unauthorized access to other computers

Can "hack" his or her way through the security levels of a computer system or network.

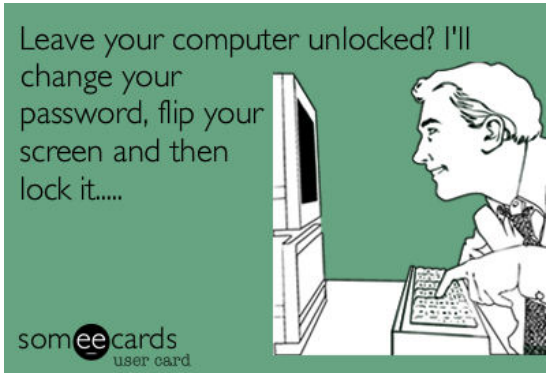


What do hackers want?

- Passwords and Account logins.
- Credit Card Numbers.
- E-mail and online-chat archives.
- Customer Information
- Pricing and Product Costs.
- Software Source Codes.
- Personal Information.

How do intruders break into your computer?

1. Send you **email** with a **virus**. Reading that email activates the virus.
2. Take advantage of a flaw or weakness in one of your computer's programs – a **vulnerability** – to gain access.
3. Once they're on your computer, they often install new **programs** that let them continue to use your computer – even after you plug the holes they used to get onto your computer in the first place. These **backdoors** are usually cleverly disguised so that they blend in with the other programs running on your computer



Crackers (‘black hats’)

- Bad people who cause trouble…
- e.g. crash machines, release computer viruses, steal credit card numbers, make free long distance calls, remove copy-protection, and distribute pirated software
- No hang-ups about stealing data

“Hack to steal and steal to hack”

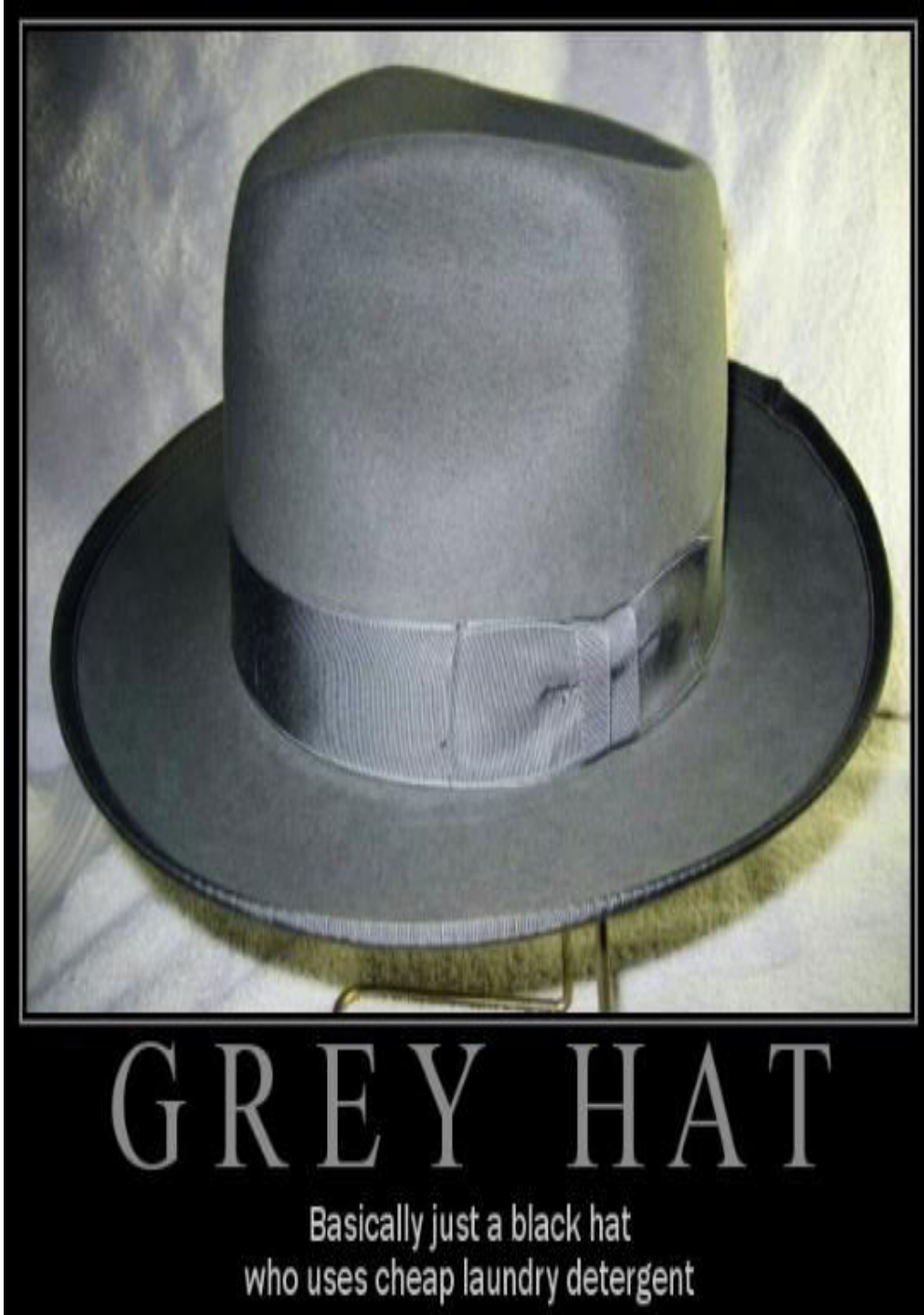
Hackers ('white/ethical hats')

- Wants to gain as much knowledge as they can about computers.
- They want to see how far they can go with their capabilities.
- They might discover holes within systems and the reasons for such holes.
- Never intentionally damage data.
- There is NO illegality involved with being a hacker
- Hackers generally deplore cracking.

Crackers are hackers, but not all hackers are crackers

Grey Hat Hacker

- Hacker of ambiguous ethics and/or borderline legality
- A mixture of white and black, these hackers can either do both white and black hat hacking, or black hat hacking and then white hat hacking



Blue Hat Hacker

- Someone outside computer security consulting firms that are used to bug test a system prior to its launch
- Look for exploits so they can be closed

Hacktivist

Hacker who utilizes technology to announce a political message.

Julian Assange founder of Wikileaks

Malware

- Combination of the words “Malicious” “software.”
- Umbrella term to refer to all sorts of software that are annoying, damaging, or intended to deceive
- e.g. spyware, adware, viruses, and worms

Self-replicating malware actively attempts to propagate by creating new copies, or instances, of itself.

Malware may also be propagated passively, by a user copying it accidentally but this isn't self-replication.

Virus

- Line of code or a function within a larger computer program
- Somebody somewhere wrote it
- Has two jobs
  - Replicate: makes copies of itself to disks
  - Activate: does something bad e.g. erase a file.
- Many viruses are simply annoyances, but some can permanently corrupt your files, destroy hard drives

Needs human action to spread e.g. floppy disk back in the day, email attachments i.e. does not replicate across networks.

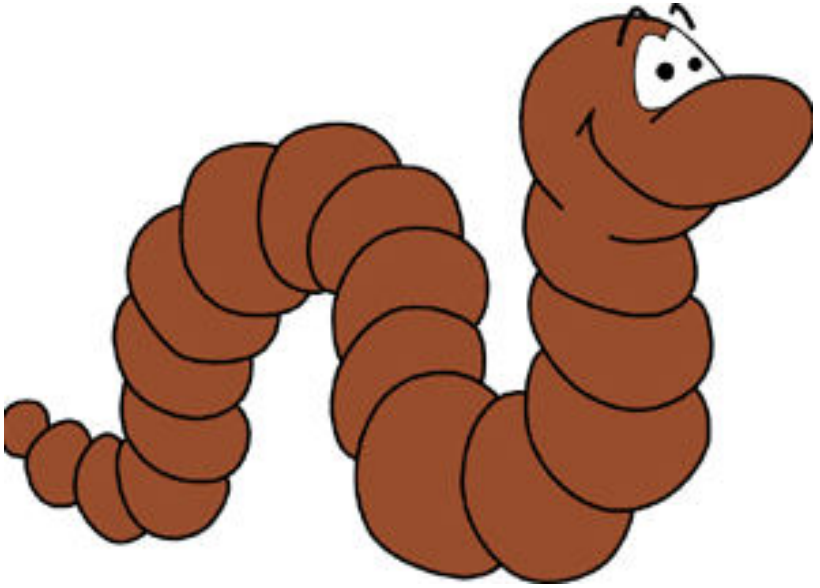
A virus isn’t a computer bug

Trojan Horses

- A malicious program disguised as a normal application e.g. someone may offer you a “free” game e.g. poker
- Looks like something harmless but is actually quite evil

Worms

- Virus that spreads itself, from file to file and from computer to computer (across the network)
- Identical in function to a virus but replicates exclusively through networks
- If the infected computer is on the network, the worm will sends out copies of itself to any other computers on the network that it can locate.



Bombs

- Part of the virus is what does the damage
- Waits for some date or event, and then does its damage

Bacteria or Rabbit programs

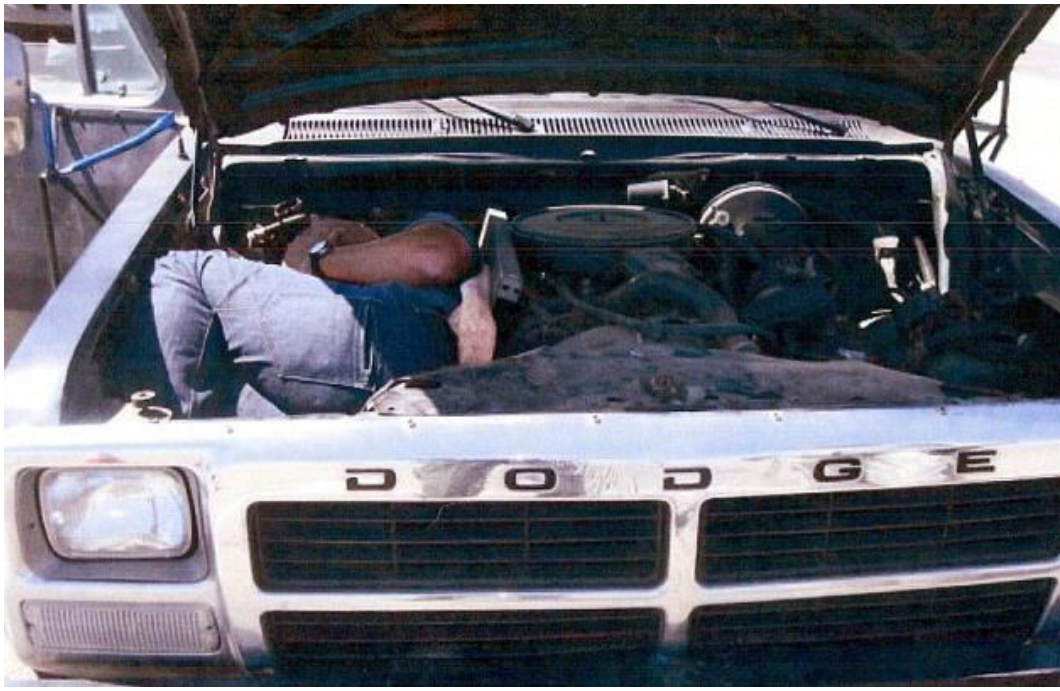
- Make copies of themselves to overwhelm a computer system's resources
- Do not damage any files
- Sole purpose: replicate themselves.

Ransom-Ware

- Gets you to down load software through a phishing scheme and then encrypts all of your files and shares so you cannot get at them.
- They will then turn around and charge a hefty fee (in the thousands) to decrypt your software for you to be able to get at it

Dropper

- Program that is not a virus, nor is it infected with a virus
- When run it installs a virus into memory, on to the disk, or into a file.

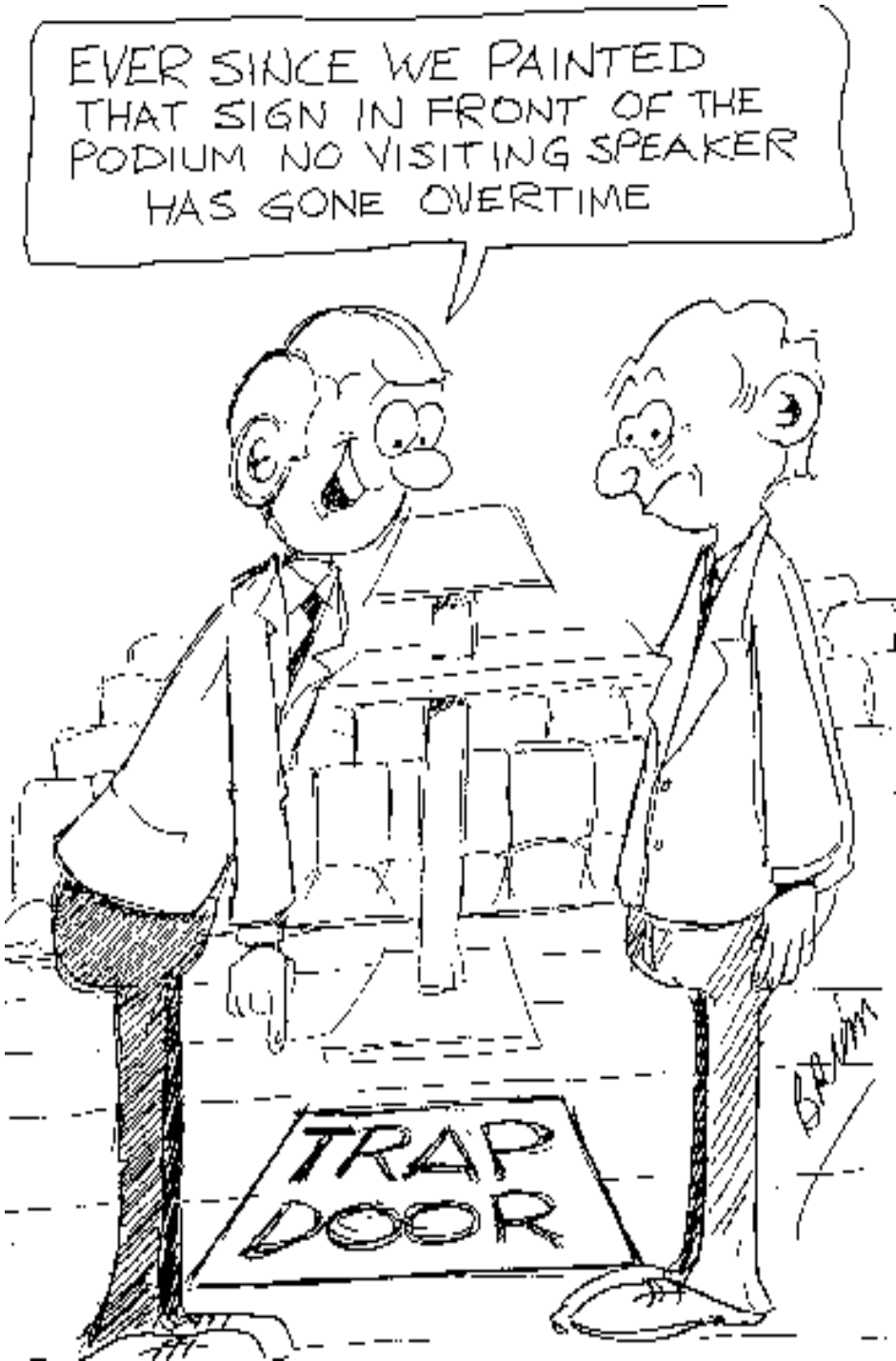


Macro Virus

- 75% of all viruses today are macro viruses
- Once on your machine, it can embed itself in all future documents you create with the application e.g. Word, Excel
- Open a document with Macro and you've got it.
- Easy to spread & learn
- e.g. March, 1999 was the Melissa virus

Trapdoor or Backdoor

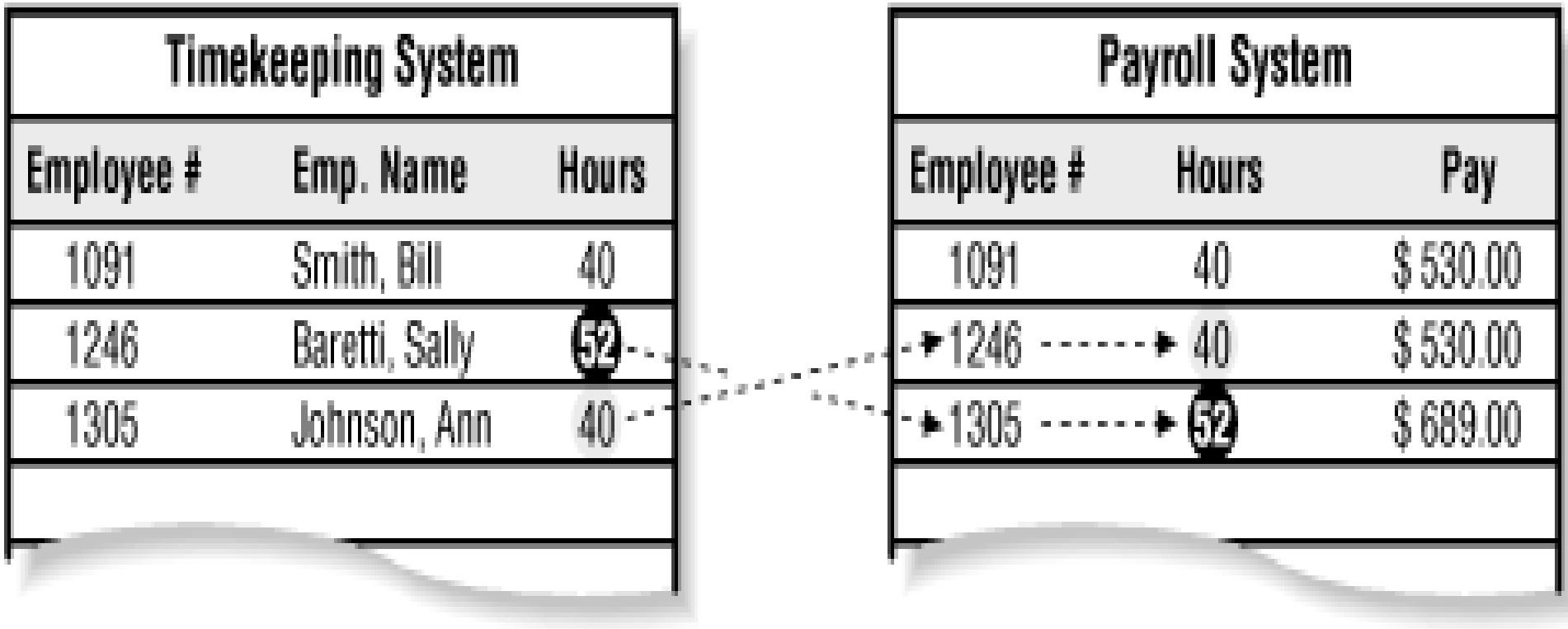
Secret/undocumented means of getting into a computer system



Dumpster Diving

Hacker goes through the garbage looking

Data Diddling: hacker that changes or forges information in an electronic resource



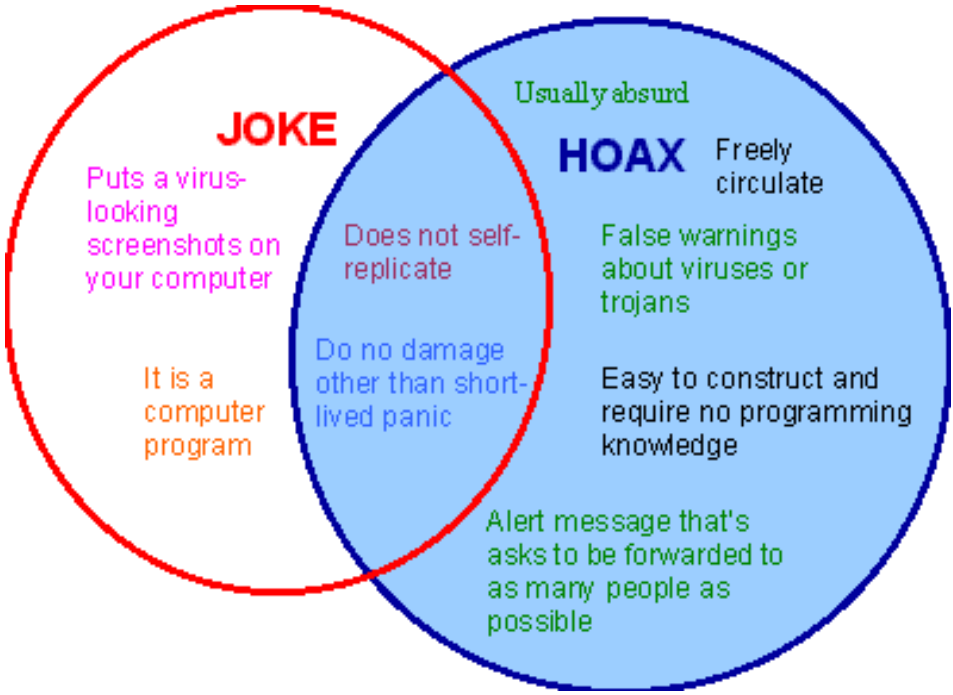
Employee numbers were switched so overtime was credited to wrong employee.

Retrovirus

Virus that actively attacks an anti-virus program or programs in an effort to prevent detection

Virus Hoax

- Email that provides a warning about a virus, worm or some other disaster, and urges recipients to forward the message
- Often sent from what appears to be a reliable source,
- e.g. McDonalds screensaver and Merry Xmas



Polymorphic

Viruses that change their characteristics i.e. change its signature to prevent detection by antivirus programs

Anti-Virus Software

- Used as both a preventative tool and as a reactive tool.
- Prevents infection and detects, and removes, viruses, worms and Trojan horses.
- Should be installed on all computers connected to the network.

Features of Anti-virus programs

1. Email checking - Scans incoming and outgoing emails, and identifies suspicious attachments.
2. Resident dynamic scanning - Checks executable files and documents when they are accessed.
3. Scheduled scans - Virus scans can be scheduled to run at regular intervals and check specific drives or the entire computer.
4. Automatic Updates - Checks for, and downloads, known virus characteristics and patterns. Can be scheduled to check for updates on a regular basis.

Spyware

- Loaded onto your system without your permission i.e. YOU do NOT install it
- Monitor actual computer activity e.g. log your keystrokes, making lists visited websites
- Once collected, the program sends this information to someone

Cookies (Web or Browser Cookie)

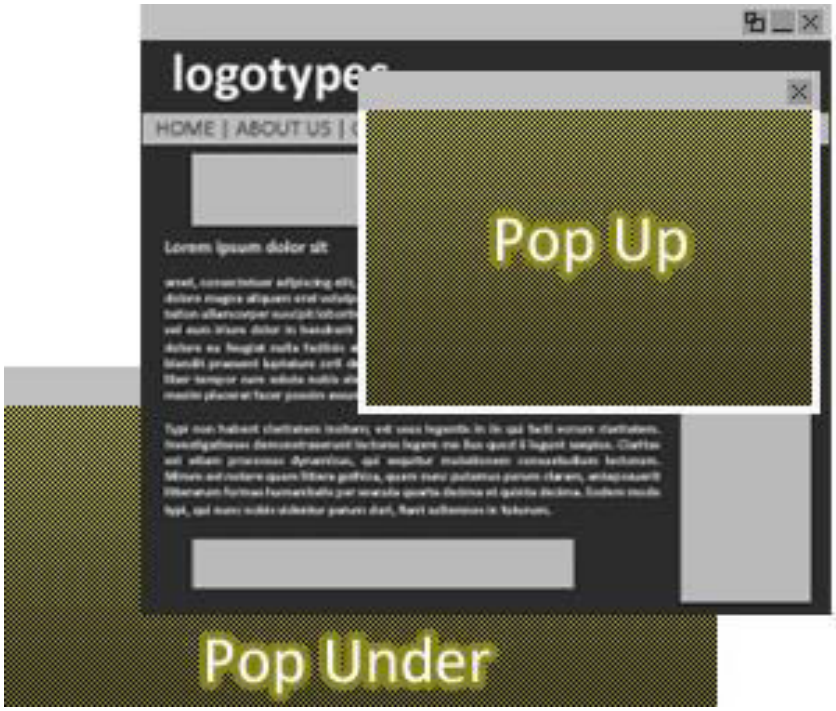
- Form of spyware but are not always bad.
- They are used to record information about visited Web Sites
- May be useful or desirable by allowing personalization and other time saving techniques.

Adware

- Software which delivers ads to your computer ads (pop-us) as you surf i.e. targeted advertising.
- Commonly installed by a user in exchange for a "free" product.

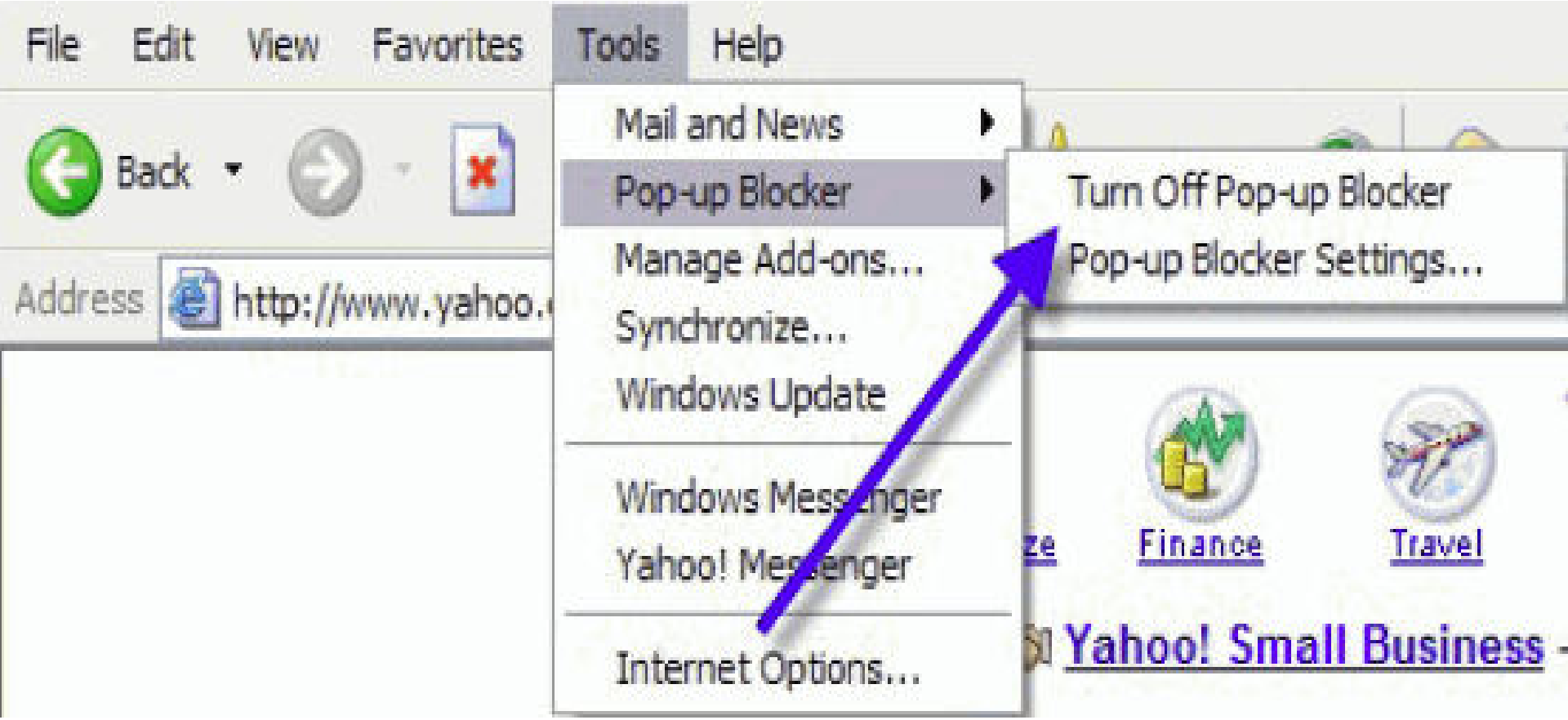
Popups and Pop Under

- Not intended to collect information about the user and are typically associated only with the web-site being visited.
- Popups: open in front of the current browser window.
- Pop Unders: open behind the current browser window..

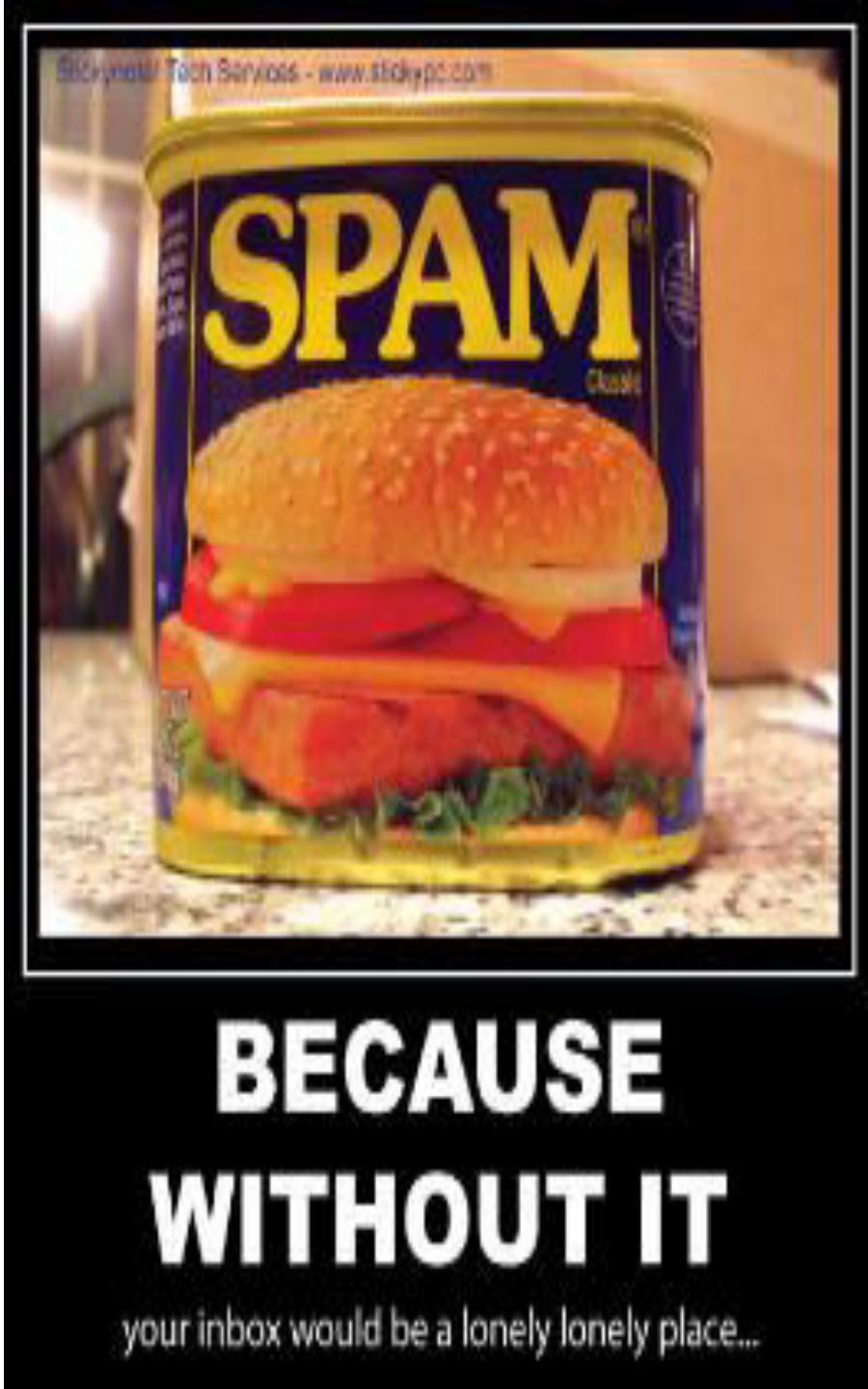


Popup Stopper Software

- Installed to prevent popups and pop under
- Many web browsers include a popup blocker feature by default.



- Sometimes merchants do not want to bother with targeted marketing.
- Send their email advertising to as many end users as possible i.e. distributed approach to marketing is **spam**



Spam

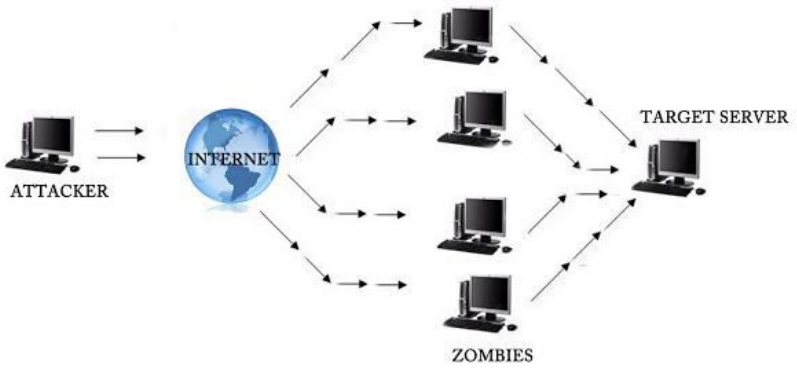
- Serious network threat that can overload ISPs, email servers and individual end-user systems.
- A person or organization responsible for sending spam is called a **spammer**.
- Spammers often make use of unsecured email servers to forward email.

70% of email traffic currently falls into this category, the spam

- Virus warning is one of the most common types of spam
- Create problems because people warn others of the impending disaster and so flood the email system.

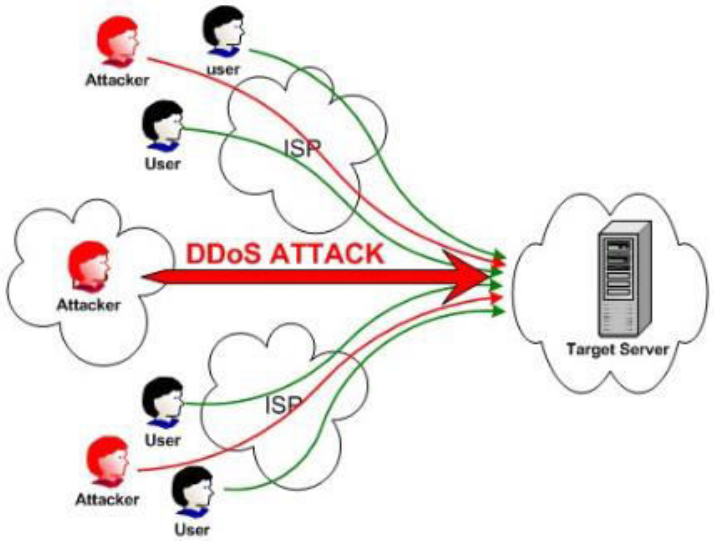
Denial of Service (DoS) attack

- Attack on a network that is designed to bring the network to its knees by flooding it with useless traffic
- Flood of messages that drastically slow down its response time, or overwhelm its data handling capacity resulting in a system crash



Distributed denial-of-service (DDoS),

- Attacker may use your computer to attack another computer.
- He or she could then force your computer to send huge amounts of data to a web site or send spam to particular email addresses.
- The attack is "distributed" because the attacker is using multiple computers, including yours, to launch the denial-of-service attack.

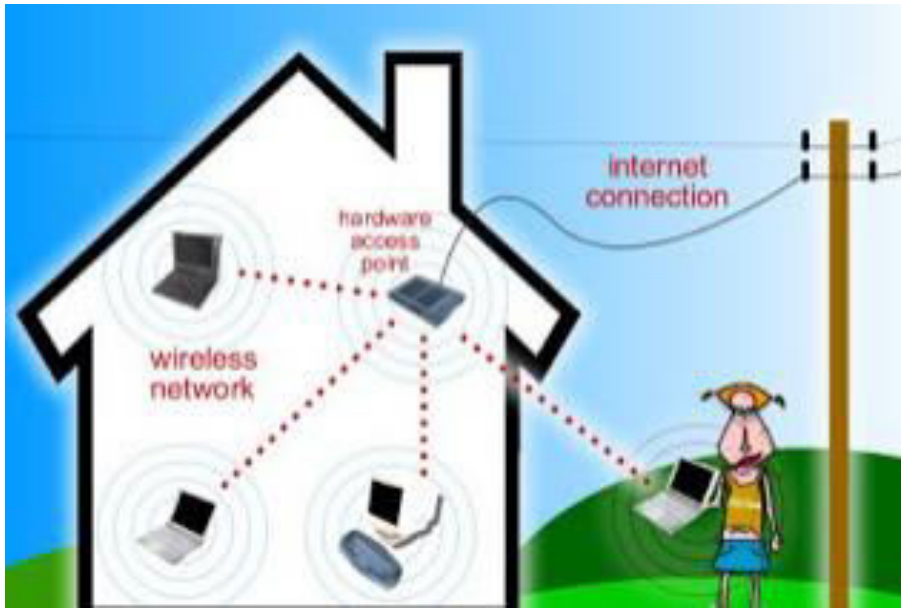


Packet Sniffing

- Act of capturing packets of data flowing across a computer network e.g. passwords, IP addresses
- To computer networks what wire tapping is to a telephone network.
- Legitimate uses: monitor network performance or troubleshoot problems with network

Piggybacking

- Connect to an unrestricted wireless network that is NOT your own
- Taking advantage of a wireless hotspot near a home or small business that does not have a secure connection



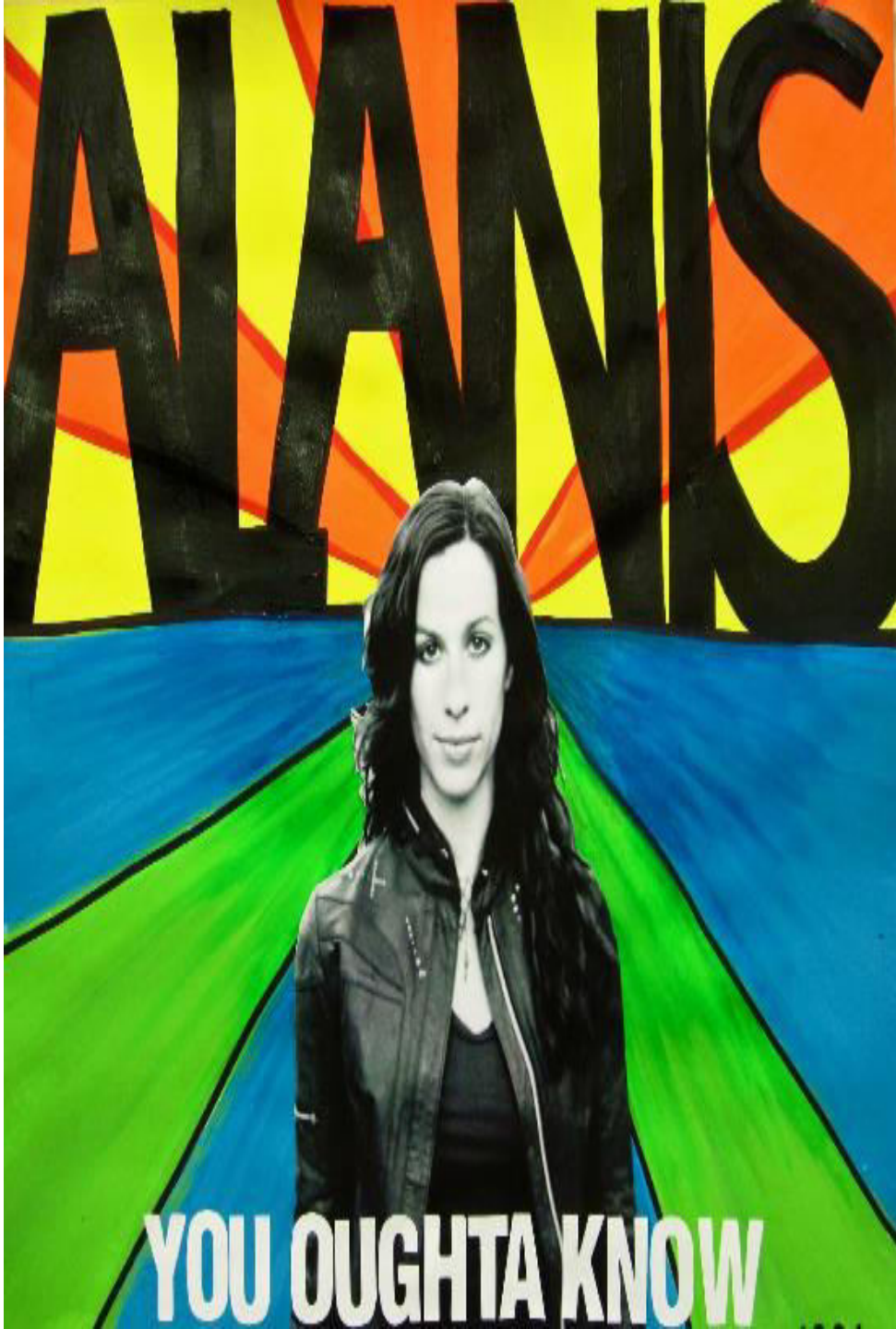
Things you ought to know

Email, instant messaging, and most web traffic go across the Internet *in the clear*

Anyone who can capture that information can read it

Things you ought to do

Always select and use strong passwords and exercise due care when reading all emails



Things you ought to install

Add a firewall, an anti-virus program, patches, and file encryption
To improve the level of security on your home computer

Security Policy

- Formal statement of the rules that users must adhere to when accessing technology and information assets.
- Can be as simple as an acceptable use policy, or can be several hundred pages in length, and detail every aspect of user connectivity and network usage procedures

Security Policy

1. Identification and Authentication Policies
2. Password Policies
3. Acceptable Use Policies
4. Remote Access Policies
5. Network Maintenance Procedures
6. Incident Handling Procedures


I HAVE NOTHING
MORE TO ADD