



Privacy, Security & Ethics

Muhammad Shafiq Hanif bin Mohamad

Manfred John Jason Dass

Noor Arinie binti Norhalil

Li ZhaoSong

Learning Objectives

- Identify the most significant concerns for effective implementation of computer technology.
- Discuss the primary privacy issues of accuracy, property and access.
- Describe the impact of large database, private networks, the Internet and the Web on privacy.
- Discuss online identity and major laws on privacy.
- Discuss about cybercrime.
- Detail ways to protect computer security.
- Discuss computer ethics

WHAT is PRIVACY ?

- **Privacy** assures that personal information (and sometimes corporate confidential informations well) are collected, processed, protected and destroyed legally and fairly.
- **Privacy** - concern the collection and use of data about individuals
- **Three primary privacy issues :**
 - **Accuracy** – responsibility of those who collect data
 - **Property** – who owns data and who has rights to software
 - **Access** – responsibility of those who control data and use of data

The Impact of Technologies Toward People

Technologies today bring a lot of positivity to people around the world, but some might also impact the negativity.

Most significant concerns :

- Privacy
 - Privacy – concerns the collection and use of data about individuals
 - Three primary privacy issues:
 - ❑ Accuracy – responsibility of those who collect data
 - ❑ Property – who owns data and who has rights to software
 - ❑ Access – responsibility of those who control data and use of data
- Security
 - Security-the access and control over sensitive information, hardware and software
- Ethics
 - The consequences that will effect society

Large Database

There are 2.5 quintillion bytes of data created each day.

- 1.7 mb per sec/per person around the world
- Mostly on mobile devices

Large organizations compile information about us daily

❑ Big Data is exploding and ever-growing

- 90% of the data collected has been collected over the last 2 years
- The amount of data increases as technologies advances (more tech/internet user)

❑ Who collects the data?

- Government agencies
- Telecommunication companies
- Credit card companies
- Supermarket scanners
- Financial institutions
- Search engines
- Social networking sites

PREDICTING PERSONAL ATTRIBUTES FROM FACEBOOK LIKES

PREDICTED ATTRIBUTE	ACCURACY
Ethnicity	95 %
Gender	93 %
Sexual Orientation (male)	88 %
Political Views	85 %
Religion	82 %
Sexual Orientation (female)	75 %
Nicotine Usage	73 %
Alcohol Usage	70 %
Relationship	67 %
Drug Usage	65 %
Parents Divorced	60 %

Predicting personal attributes from Facebook Likes. Source: Kosinski et al 2013.

PREDICTING CHARACTER TRAITS FROM PHONE CALL RECORDS AND APP USAGE

Source: Chittaranjan et al, 2011



RECOGNIZING EMOTIONS FROM THE RHYTHM OF KEYBOARD TYPING PATTERNS

Source: Epp et al, 2011

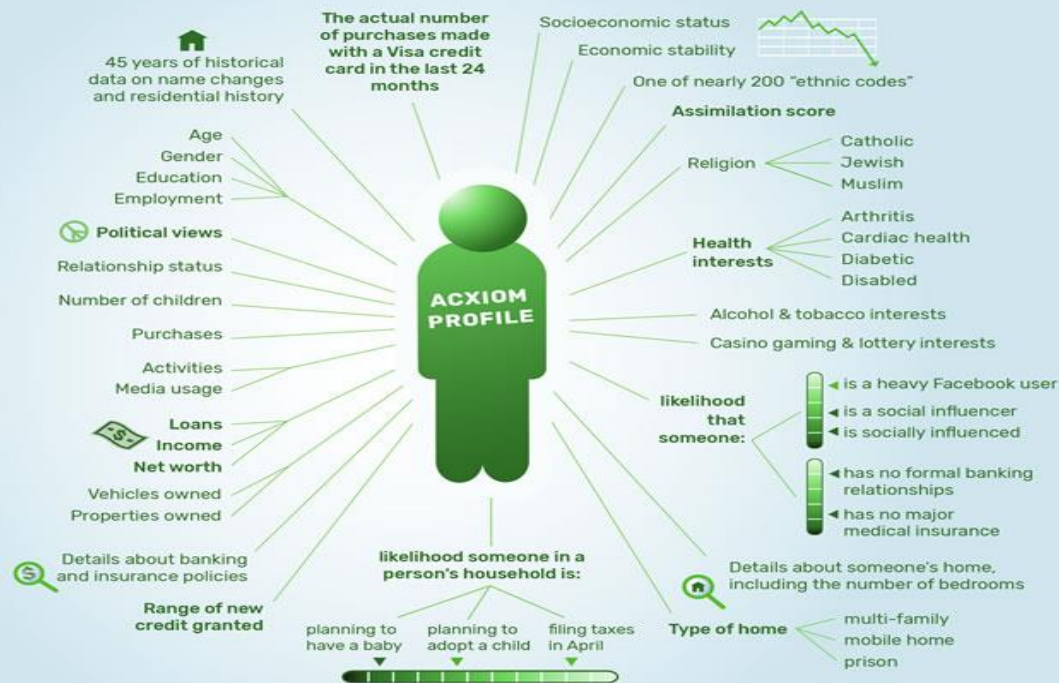


Information Resellers/Brokers

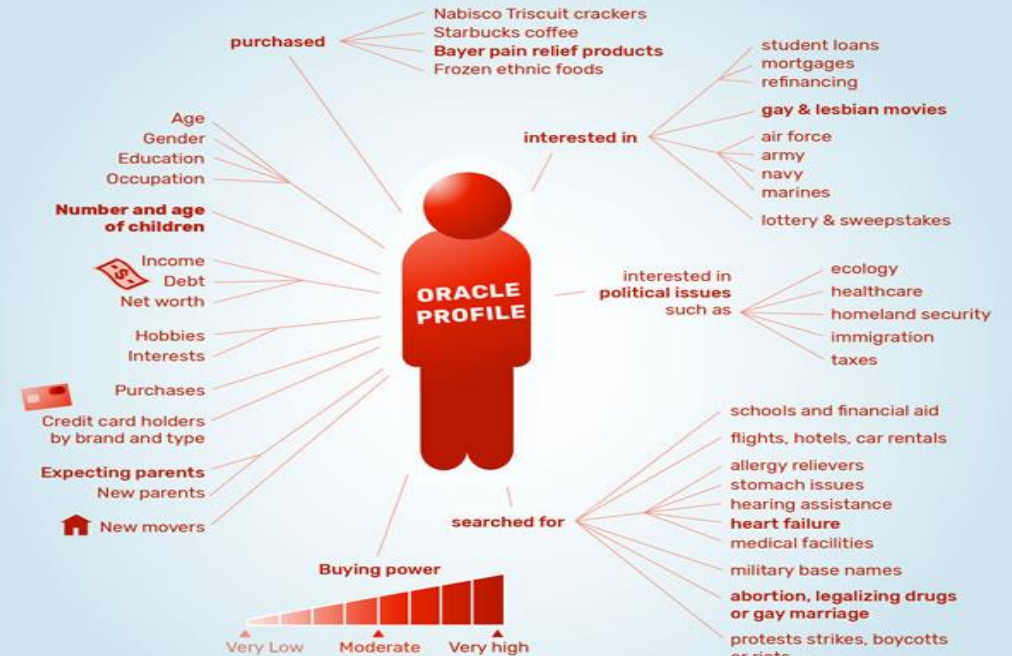
- Collect and sell personal data
- Create electronic profiles

DATA BROKERS HAVE EXTENSIVE PROFILE INFORMATION ON ENTIRE POPULATIONS

Examples of data on consumers provided by Acxiom and Oracle



Acxiom provides up to 3,000 attributes and scores on 700 million people in the US, Europe, and other regions.



Oracle sorts people into thousands of categories and provides > 30,000 attributes on 2 billion consumer profiles

❑ Personal information is a marketable commodity, Risk?

- Collecting public, but personally identifying information (Name, address,..etc)
- Spreading information without personal consent, leading to identity theft
- Spreading inaccurate information

❑ Freedom of Information Act

- Law that allow access by the general public to data held by national governments
- Increasing dissatisfaction with the secrecy surrounding government policy development and decision making

Private Networks

- A network which access is restricted and tightly controlled (opposite to public network)
- Example :
 - ✓ Corporate network
 - ✓ School network
- Some of people's corporate privacy
 - ❑ Employers can monitor e-mail legally
 - A proposed law could prohibit this type of electronic monitoring or at least require the employer to notify the employee first



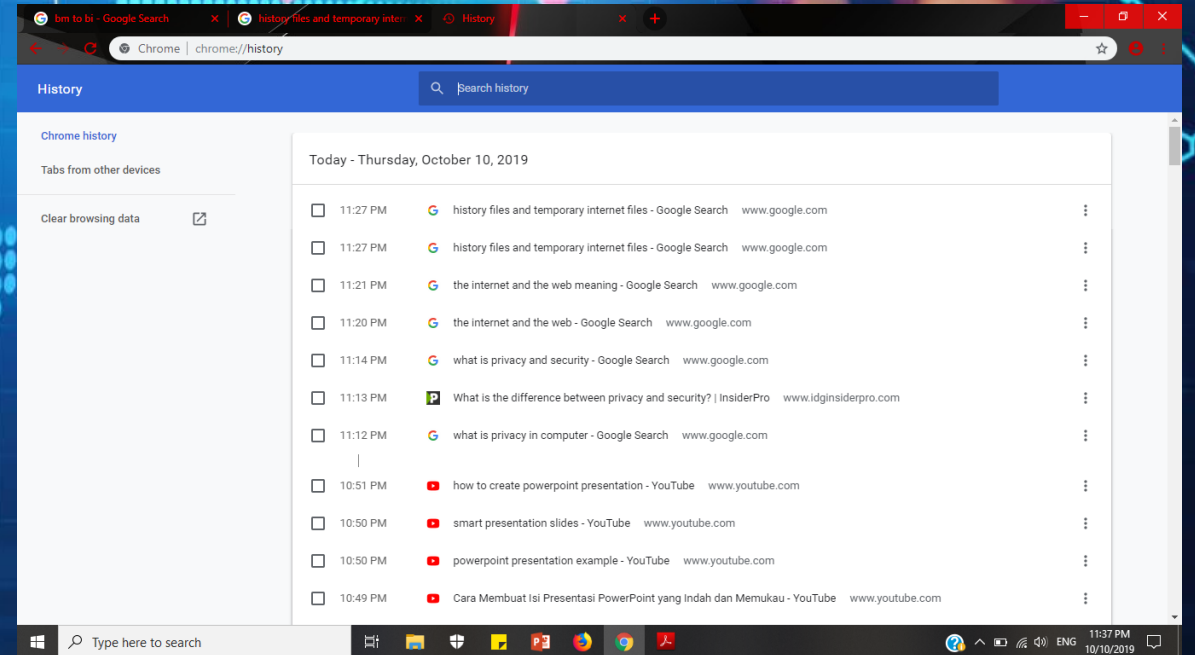
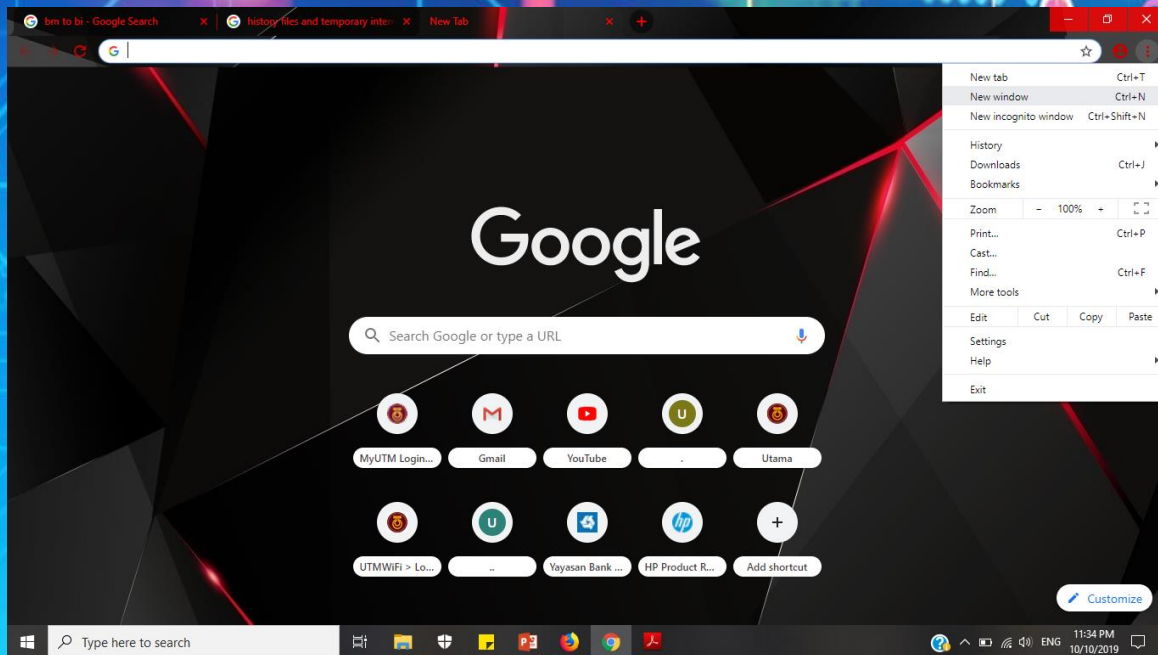
ENCRYPTED CONNECTION

The Internet and the Web

- **The Internet** is a global network of networks while the **Web**, also referred formally as World Wide **Web** (www) is collection of information which is accessed via **the Internet**.
- **Illusion of anonymity** – People not concerned about privacy when surfing the Internet or when sending e-mail.
- **When browsing the web, critical information is stored on the hard drive in these locations :**
 - History Files
 - Temporary Internet Files
 - Cookies
 - Privacy Mode

History Files and Temporary Internet Files

- History Files
 - Include locations or addresses of sites you have recently visited
- Temporary Internet Files / Browser Cache
 - Saved files from visited websites
 - Offers quick re-display when you return to the site



What Is a Cookie?

- Cookie is data stored by the browser on behalf of a web server
- A browser sends Cookies with every request to the corresponding web server
- Cookies are small data files that are deposited on your hard disk from web sites you have visited

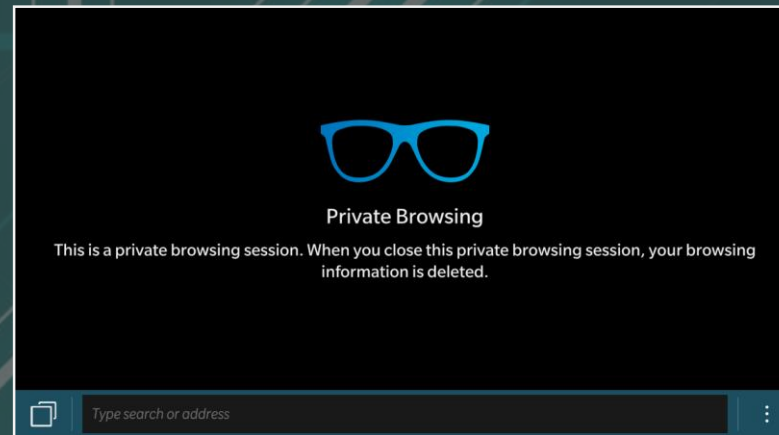


- First-party cookies are generated only by websites you are visiting
- Third-party cookies are generated by an advertising company that is affiliated with the website

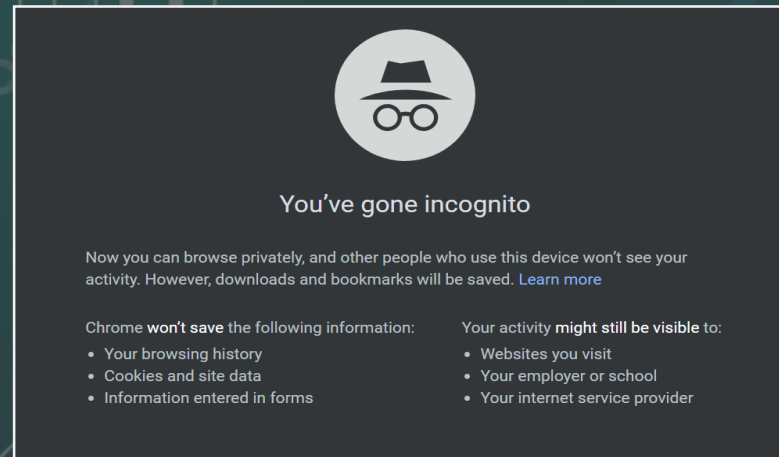
Private Modes

- Ensure your browsing activity is not recorded on your hard drive

- Private Browsing



- Incognito Mode



Privacy Threats

WEB BUGS

- Also known as a Web beacon, is a file object that is placed on a Web page or in an email message to monitor user behavior.
- When a user opens the message information is sent back to the source of the bug

A web bug can gather the following information :

- The IP address of the computer that fetched the Web bug.
- The URL of the page that the Web bug is located on.
- The URL of the Web bug.
- The time the Web bug was viewed.
- The type of browser that fetched the Web bug.
- A previously set cookie value.

SPYWARE

- Unwanted software that infiltrates your computing device, stealing your internet usage data and sensitive information.
- Spyware gathers your personal information and relays it to advertisers, data firms or external users.

There are four main types of spyware :

1. **Adware.** This type of spyware tracks your browser history and downloads. Adware is used for marketing purposes and can slow down your computer.
2. **Trojan.** This kind of malicious software disguises itself as legitimate software. It can be used to access sensitive information such as Social Security numbers and credit card information.
3. **Tracking cookies.** These track the user's web activities, such as searches, history and downloads for marketing purposes.
4. **System monitors.** This type of spyware can capture just about everything you do on your computer. System monitors can record all keystrokes, emails, chat-room dialogs, websites visited and programs run.



Some of the most common ways your computer can become infected with spyware include these :

- i. Accepting a prompt or pop-up without reading it first
- ii. Downloading software from an unreliable source
- iii. Opening email attachments from unknown senders
- iv. Pirating media such as movies, music or games

ANTI-SPYWARE SOFTWARE

- Anti-spyware software is a type of program designed to prevent and detect unwanted spyware program installations and to remove those programs if installed.
- Detects spyware through rules-based methods or based on downloaded definition files that identify common spyware programs.
- Can act much like an anti-virus program by providing real-time protection and preventing spyware from being downloaded in the first place.

A few examples of anti spyware software :

1. Bitdefender Antivirus
2. Avira Free Security Suite
3. AVG AntiVirus
4. Malwarebytes Anti-Malware
5. SpyBot Search & Destroy
6. Emsisoft Emergency Kit
7. Avast Anti-Virus

Online Identity

- Also known as Internet identity (IID), online identity or internet persona.
- Is a social identity that Internet user voluntarily makes available in online communities and websites such as social media platforms.
- Archiving and search features of the Web make it available indefinitely.

An Internet identity can even be comprised of things like :

- ✓ Login credentials
- ✓ Online transactions
- ✓ Online search activities
- ✓ Medical history
- ✓ Date of birth
- ✓ Browsing history

Some of the entities that are interested in your private data, identity, web traffic, Internet usage habits and other sensitive information include :

- Your ISP
- Hackers
- Advertisers
- Government surveillance agencies
- The authorities
- Search engines and social media platforms
- Any other websites you visit
- All sorts of businesses

Major Laws on Privacy :

- *Gramm-Leach-Bliley Act protects personal financial information*
- *Health Insurance Portability and Accountability Act (HIPAA) protects medical records*
- *Family Educational Rights and Privacy Act (FERPA) resists disclosure of educational records*

WHAT is Security ?

- Computer **security**, cybersecurity or information technology **security** (IT **security**) is the protection of computer systems from the theft of or damage to their hardware, software, or electronic data, as well as from the disruption or misdirection of the services they provide.
 - Hackers
 - Gains unauthorized access with malicious intent
 - Not all hackers are illegal
 - Cybercrime / Computer Crime
 - Criminal offense that involves a computer and a network

Forms of Computer Crime

Computet Crime	Description
Malicious programs	Include viruses, worms and Torjan horses
DoS	Causes computer systems to slow down or stop
Rogue WIFI hotspots	Imitate legitimate WIFI hotspot in order to capture personal information
Data manipulation	Involves changing data or leaving prank messages
Identity theft	Is illegal assumption of a person's identity for economic gain
Internet scams	Are scams over the Internet usually initiated by e-mail and involving phishing
Cyberbullying	Is using the Internet, smartphones or other devices to send/post content intended to hurt or embarrass another person

Malicious Programs - Malware

- **Viruses**

- A computer virus is a type of computer program that, when executed, replicates itself by modifying other computer programs and inserting its own code. When this replication succeeds, the affected areas are then said to be "infected" with a computer virus

- **Worms**

- A computer worm is a standalone malware computer program that replicates itself in order to spread to other computers.
- Worms almost always cause at least some harm to the network, even if only by consuming bandwidth, whereas viruses almost always corrupt or modify files on a targeted computer.

Cyber Crime

- **Cybercrime** is defined as a **crime** in which a computer is the object of the **crime** (hacking, phishing, spamming) or is used as a tool to commit an offense (child pornography, hate **crimes**).
- Denial of Service
 - (DoS) attack attempts to slow down or stop a computer system or network by flooding it with requests for information or data
- Rogue Wi-Fi hotspots
 - Imitate free Wi-Fi networks and capture any and all information sent by the users to legitimate sites including usernames and passwords
- Data manipulation
 - Finding entry into someone's computer network and leaving a pranksker's message



• Trojan horse

- In computing, a Trojan horse, is any malware which misleads users of its true intent.
- From Greek story of deceptive Trojan Horse-Disguised as normal software
- Spread by hacker/email attachment.

Internet Scams

A fraudulent or deceptive act or operation to trick someone into providing personal information or spending money for little or no return

- Identity Theft
 - Illegal assumption of someone's identity for purpose of economic gain
- Cyber-bullying
 - Use of the Internet, cell phones or other devices to send or post content intended to harm
- Phishing
 - Attempts to trick Internet users into thinking a fake but official-looking website is legitimate

Types of Internet Scams

Type	Description
Chain letter	Classic chain letter instructing recipient to send a nominal amount of money to each of five people on a list. The recipient removes the first name on the list, adds his or her name at the bottom and mails the chainletter to five friends. This is also known as a pyramid scheme. Almost all chain letters are fraudulent and illegal.
Auction fraud	Merchandise is selected and payment is sent. Merchandise is never delivered.
Vacation prize	“Free” vacation has been awarded. Upon arrival at vacation destination, the accommodations are dreadful but can be upgraded for a fee.
Advance fee loans	Guaranteed low-rate loans available at almost anyone. After applicant provides personal loan-related information, the loan is granted subject to payment of an “insurance fee”.

Measures to Protect Computer Security

Principle measures to ensure computer security

- Restricting access – Limit access to authorized persons using such measures as passwords and firewalls
- Encrypting data – Code all messages sent over a network
- Anticipating disasters – Prepare for disasters by ensuring physical security and data security through a disaster recovery plan.
 - Physical security
 - Data security
 - Disaster recovery plan
- Preventing data loss – Routinely copy data and store it at a remote location.

Restricting Access

- **Biometric scanning**

- Fingerprint scanners
- Iris (eye) scanners

- **Passwords**

Dictionary attack

- Uses software to try thousands of common words sequentially in an attempt to gain unauthorized access to a user's account.

So, there is still a risk to crack password. We have to set the limitation on numbers of times the wrong password was entered.

Automated Security Tasks

Ways to perform and automate important security tasks

- **Security Suites**

- ✓ Provide a antivirus program designed to protect your privacy and security

- **Firewalls**

- ✓ Security buffer between a corporation's provide network and all external networks

- **Password Managers**

- ✓ Helps to create strong passwords . Such as at least 8 digits with upper letter and numbers.

Encryption

- Coding information to make it unreadable, except to those who have the encryption key
- For example, E-mail encryption, File encryption, Web site encryption, Virtual private networks (VPNs), Wireless network encryption.

Anticipating Disasters

- Physical Security protects hardware
- Data Security protects software and data from unauthorized tampering or damage
 - ✓ Disaster Recovery Plan describes ways to continue operating in the event of a disaster
- Frequent backups
- Redundant data storage

Cloud-Based Backup

- Cloud-based backup services such as Carbonite , Google drive.

WHAT is ETHICS ?

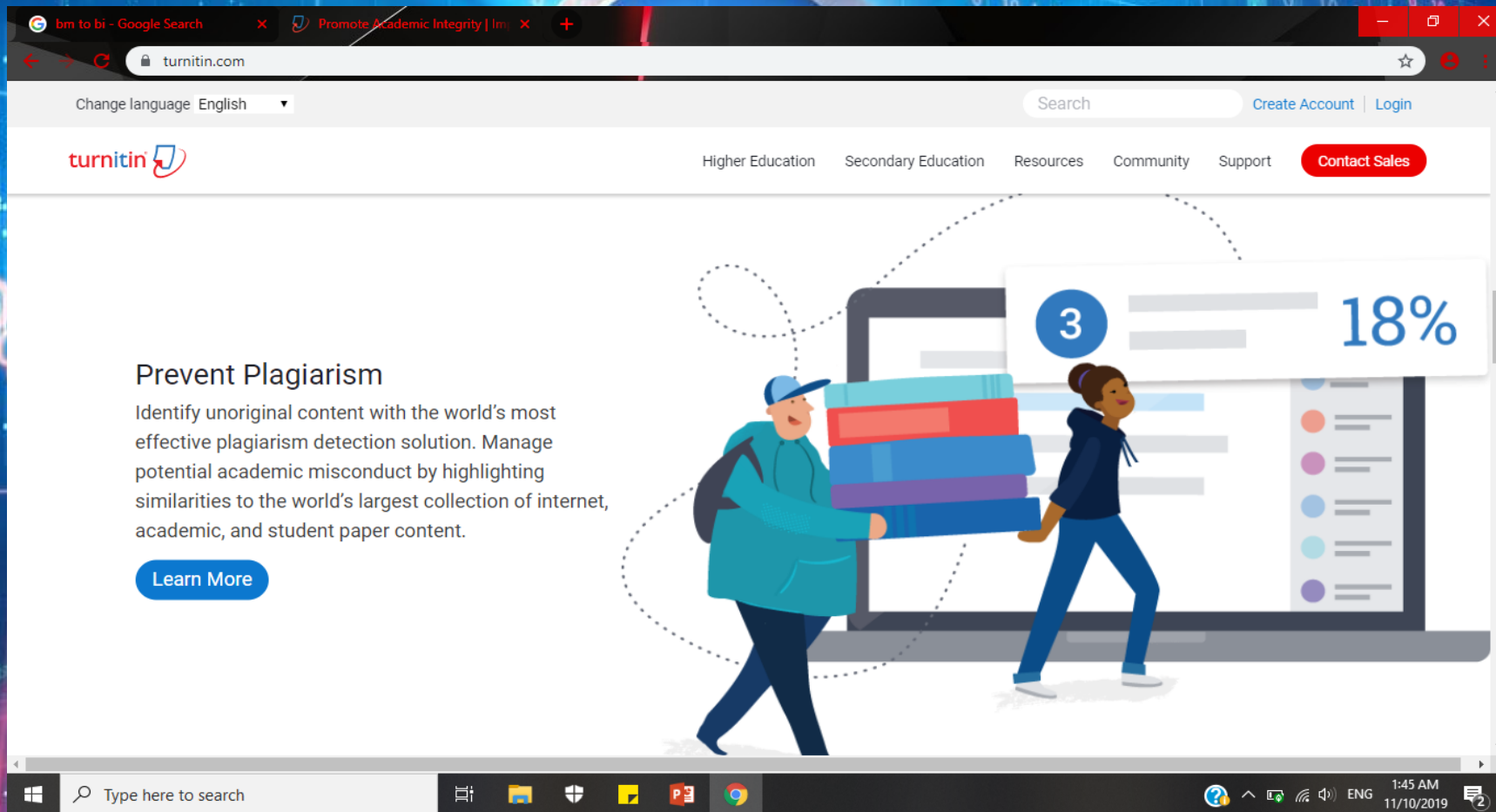
Ethics is **defined** as a moral philosophy or code of morals practiced by a person or group of people.

Computer Ethics – guidelines for the morally acceptable use of computers

- Copyright
 - Gives content creators the right to control the use and distribution of their work
 - Paintings, books, music, films, video games
- Software piracy
 - Unauthorized copying and distribution of software
 - Digital rights management (DRM) controls access to electronic media
 - Digital Millennium Copyright Act protects against piracy

Plagiarism

Representing some other person's work and ideas as your own without giving credit to the original person's work and ideas



The screenshot shows the Turnitin website interface. At the top, there's a navigation bar with the Turnitin logo, links for 'Higher Education', 'Secondary Education', 'Resources', 'Community', 'Support', and a red 'Contact Sales' button. Below this, the main heading is 'Prevent Plagiarism', followed by a paragraph: 'Identify unoriginal content with the world's most effective plagiarism detection solution. Manage potential academic misconduct by highlighting similarities to the world's largest collection of internet, academic, and student paper content.' A blue 'Learn More' button is positioned below the text. To the right, there's an illustration of two people carrying a large stack of books, with a large '3' and '18%' displayed next to them, suggesting a statistic or a count. The background of the entire image is a digital theme with binary code (0s and 1s) and glowing lines.

bm to bi - Google Search x Promote Academic Integrity | Im x +

turnitin.com

Change language English

Search Create Account Login

turnitin

Higher Education Secondary Education Resources Community Support Contact Sales

Prevent Plagiarism

Identify unoriginal content with the world's most effective plagiarism detection solution. Manage potential academic misconduct by highlighting similarities to the world's largest collection of internet, academic, and student paper content.

Learn More

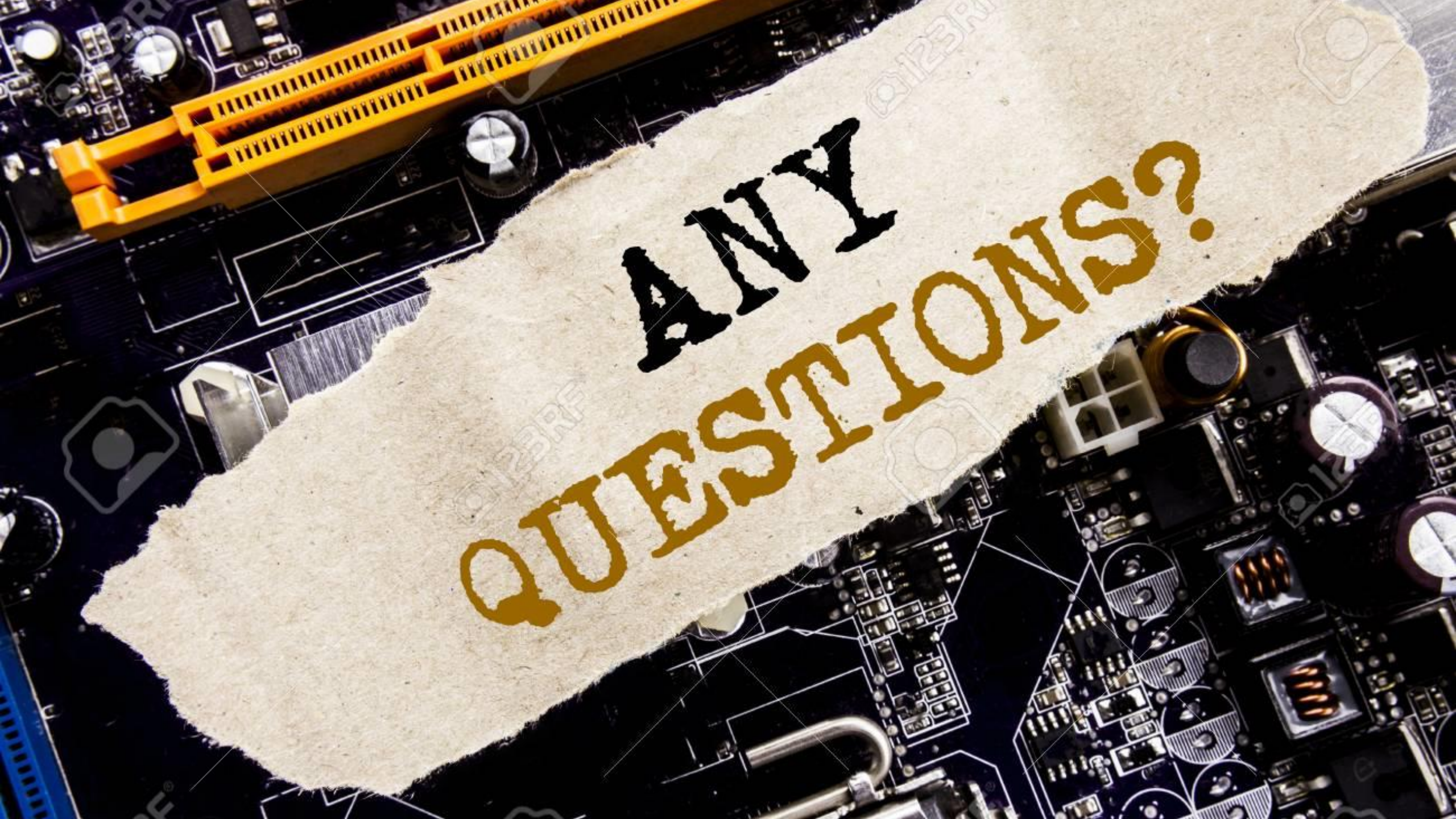
3 18%

Type here to search

1:45 AM 11/10/2019

A black and white photograph of an open laptop. The screen is the central focus, displaying the words "THE END" in a white, hand-drawn, cursive-style font. The laptop's keyboard is visible in the foreground, and the dark bezel of the screen is also visible. The background is a dark, out-of-focus surface.

THE END

A close-up photograph of a computer motherboard with a piece of torn, light-brown paper placed on top of it. The paper has the words "ANY" and "QUESTIONS?" printed on it. "ANY" is in a bold, black, sans-serif font, and "QUESTIONS?" is in a bold, yellow, sans-serif font. The motherboard is dark green or black, with various electronic components visible, including a yellow PCI slot at the top, several capacitors, and integrated circuits. The paper is torn at the edges, giving it a rough, handmade appearance. The overall image suggests a theme of technology, troubleshooting, or a quiz related to computer hardware.

ANY
QUESTIONS?