SPI GROUP 2 - BUGS

is a word used to describe problems with computers, sucj as mistakes, glitches, and errors

BUG

Types of Bugs

Functional Bugs
Logical Bugs
Syntax Errors
Compatibility Issues
User Interface Bugs

---

are associated with the functionality of a specific software component

Functional bugs

---

any component in an app or website that doesn’t function as intended is what type of bug

Functional bugs

---

disrupts the intended workflow of software and causes it to behave incorrectly

logical bug

---

primarily take place due to poorly written code or misinterpretation of business logic

logical bug

These occur when there are mistakes in the programming code, such as typos or incorrect punctuation.

Syntax Errors

These occur when software may not work as expected on different operating systems, browsers, or devices, leading to compatibility issues

Compatibility Issues

Issues with the graphical user interface, such as misaligned elements or inconsistent styling, can impact the user experience

User Interface Bugs

When was the first computer bug found?

September 9, 1947, at 3:45 p.m.

Who records ‘the first computer bug’ in the Harvard Mark II computer’s logbook and wrote it as “First actual case of bug being found.”

Grace Murray Hopper

---

examples of how bugs can impact public safety include

Software Vulnerabilities
Security Vulnerabilities
Internet of Things (IoT) Devices
Autonomous Vehicles
Medical Device Software
Air Traffic Control Systems
Public Safety Communications Systems
Public Infrastructure

---

encourages creating failing tests for the feature/product before developing the feature/product

Test-Driven Development (TDD)

---

emphasizes that every code change integrated into the central code repository should be automatically tested with predefined test cases.

Continuous Integration Continuous Testing (CICT)

---

encourages the use of a Domain Specific Language (DSL) for communication between and within teams. Using DSL helps in reducing miscommunication among stakeholders. When BDD is used, tests can be created in a simple text language like English which makes it easy for everyone in the team to participate in creating and reviewing tests without getting into the nitty-gritty of code syntax.

Behaviour Driven Development(BDD)

As the scope for the product evolves, so do specifications related to it. The dedicated effort may be required to review and track the updates happening in specifications. Early catching of any updates in the specifications which may lead to a potential conflict, can help in preventing bugs later in the implementation of the product.

Specification Review and Management

Open and clear communication among teams and team members can help a lot in highlighting absent/conflicting scenarios in specifications

Clear Communication

---

is a broad term encompassing any harmful program or code designed to harm computer systems

malicious software

---

short for "malicious software, "

Malware

Signs of Malware

The device suddenly slows down, crashes, or displays repeated error messages
Your device won’t shut down or restart
Your device won’t let you remove software
Your device serves up lots of pop-ups, inappropriate ads, or ads that interfere with page content
Your device shows ads in places you typically wouldn’t see them, like government websites

Your device shows new and unexpected toolbars or icons in your browser or on your desktop
Your device uses a new default search engine or displays new tabs or websites you didn’t open
Your device keeps changing your computer’s internet home page
Your device sends emails you didn’t write
Your device runs out of battery life more quickly than it should

---

Types of Malware

Adware
Spyware
Virus
Worms
Trojan
Ransomware
Rootkit
Keylogger
Malicious Cryptomining
Exploits

---

a type of malware similar to viruses. Like viruses, worms are self-replicating

Worms

What is the differene between Worms and Virus

The big difference is that worms can spread across systems on their own, whereas viruses need some sort of action from a user in order to initiate the infection.

---

is one of the most dangerous malware types. It usually represents itself as something useful in order to trick you. Once it’s on your system, the attackers behind the attack gain unauthorized access to the affected computer.

Trojan

---

a criminal business model that uses malicious software to hold valuable files, data, or information for ransom

Ransomware

Tojan is also known as

Trojan horse

---

a form of malware that provides the attacker with administrator privileges on the infected system, also known as “root” access. Typically, it is also designed to stay hidden from the user, other software on the system, and the operating system itself.

Rootkit

---

is malware that records all the user’s keystrokes on the keyboard, typically storing the gathered information and sending it to the attacker, who is seeking sensitive information like usernames, passwords, or credit card details

Keylogger

---

sometimes called drive-by mining or cryptojacking

Malicious Cryptomining

---

is an increasingly prevalent malware usually installed by a Trojan.

Malicious Cryptomining

It allows someone else to use your computer to mine cryptocurrency like Bitcoin or Monero.

Malicious Cryptomining

---

are a type of malware that takes advantage of bugs and vulnerabilities in a system in order to give the attacker access to your system. While there, the attacker might steal your data or drop some form of malware

Exploits

---

refers to a software vulnerability for which there is currently no available defense or fix

zero-day exploit

Malware also uses various methods to spread itself to other computer systems beyond an initial attack vector. Malware attack definitions can include:

Email attachments containing malicious code can be opened and therefore executed by unsuspecting users. If those emails are forwarded, the malware can spread even deeper into an organization, compromising a network

File servers, such as those based on common Internet file systems (SMB/CIFS) and network file systems (NFS), can enable malware to spread quickly as users access and download infected files.

File-sharing software can allow malware to replicate itself onto removable media and then onto computer systems and networks.

Peer-to-peer (P2P) file sharing can introduce malware by sharing files as seemingly harmless as music or pictures

Remotely exploitable vulnerabilities can enable a hacker to access systems regardless of geographic location with little or no need for involvement by a computer user.

How to Prevent Malware

Keep your computer and software updated
Use a non-administrator account whenever possible
Think twice before clicking links or downloading anything
Be careful about opening email attachments or images
Don ’t trust pop-up windows that ask you to download software
Limit your file-sharing
Use anti-virus software

---

is a fundamental concept that plays a crucial role in various aspects of society, including technology, government, business, and more.

Public Trust

It represents the belief, confidence, and reliance that individuals and communities have in an entity, system, or organization.

Public Trust

Importance of Public Trust

Allows people to cooperate
Encourages innovation and risk-taking.
Makes it easier to resolve disputes.
Strengthens democracy.
Promotes economic growth.
Improves overall well-being.

Factors that affect public trust

Transparency
Ethical Conduct
Ethical Conduct
Communication
Data Privacy and Security
Accountability

---

involves providing information about an organization's actions, decisions, and policies, as well as how they handle data and resources.

Transparency

Ethical behavior, including honesty, fairness, and integrity, is a cornerstone of public trust. Unethical actions can erode trust quickly

Ethical Conduct

Consistently meeting commitments and delivering on promises builds trust

Reliability

---

demonstrates that an entity is dependable and can be counted on.

Reliability

Effective and honest communication is key. This includes keeping the public informed about actions, decisions, and any changes that may affect them.

Communication

Protecting personal data and ensuring data security is essential, particularly in the digital age. Breaches of data privacy can damage trust significantly.

Data Privacy and Security

Taking responsibility for mistakes, addressing problems promptly, and being accountable for actions or decisions helps maintain trust

Accountability

This means being open and honest about the government's or institution's activities.

Being transparent

This means being held responsible for the government's or institution's actions.

Being accountable

This means being qualified to do the government's or institution's job

Being competent

This means being clear and concise in communications and being responsive to people's questions and concerns

Communicating effectively