Unauthorized access is when someone gains **access** to a website, program, server, service, or other system using someone else's account or other methods.

Unauthorized access could also occur if a user attempts to **access** an area of a system they should not be **accessing.**

How do I fix unauthorized access:

Use Strong Passwords

1. Use antivirus software. “Do not avoid security patches”. ...
2. Keep the software up to date.
3. Verify your software security. Do not allow any application to make changes to your computer.
4. Back up early and often. Make use of websites that provide storage and allow you to keep a copy of your information.

Unauthorized access means trespassing into a computer without consent, and retrieving data, storing data, communicating with, intercepting, or changing data or software. Hacking is breaking into a computer system with the intention of maliciously altering, damaging, or disrupting the computer system or networks.

5 Common Types of Unauthorized Access and How to Combat Them

- Tailgating. One of the most common types of unauthorized access is tailgating, which occurs when one or more people follow an authorized user through a door. ...
- Door Propping. ...
- Levering Doors. ...
- Keys. ...
- Access Cards.

UNAUTHORIZED ACCESS - use of a computer or network without permission. ... **UNAUTHORIZED USE- Use** of a computer or its data for unapproved or illegal activities. - Ex: gaining **access** to a bank computer and performing an **unauthorized** bank transfer etc.

Trojans, viruses, spyware, and other malware **can** monitor your **computer** and log keystrokes to capture sensitive data, such as passwords and credit card information. To help protect your **computer** from these threats, we suggest installing antivirus and anti-spyware protection programs.

The Three Types of Access Control Systems

Access control systems come in **three** variations: Discretionary **Access Control** (DAC), Mandatory **Access Control** (MAC), and Role-Based **Access Control** (RBAC).

Unauthorized access is when someone gains **access** to a website, program, server, service, or other system using someone else's account or other methods. For example, if someone kept guessing a password or username for an account that was not theirs until they gained **access**, it is considered **unauthorized access**

Laptop and Mobile Device Theft

Laptops and other portable devices (such as tablets, smart phones, USB drives, CDs, floppy disks, etc.) are frequently stolen or lost. Remember that you should eliminate any unauthorized sensitive information from portable devices and encrypt all authorized sensitive information.

Follow these steps to protect your devices.

1. **Physically secure your laptop** computer by keeping it in an office that can be locked. Also, use a cable lock to secure it to a desk or heavy object in or outside of the office.
2. The University Police department offers a **laptop registration and engraving service** called Operation ID to help identify stolen equipment.
3. **Do not store sensitive or confidential data** on mobile devices unless you have been authorized to do so.
4. **Avoid leaving your mobile devices and media unattended.**
5. **Always use a password** to protect your portable device against unauthorized use.
6. **Turn Bluetooth power off** by default, and do not let it be set to discoverable.
7. **Turn off the radio switch** for your laptop's Wi-Fi access when you are not using it.
8. **If a portable device is lost or stolen, contact University Police for assistance.**