Physical Computer Security

What Is Physical Computer Security?

Devices that access critical corporate information must be protected in order to prevent this information from ending up in the wrong hands. Here is a list of common items that need to be protected in the workplace:

Laptops	•Secure your laptop with a cable lock while you are away from your desk to prevent theft. Lock your laptop with a password to prevent others from logging on to your computer.
Desktops	•Desktops are larger and harder to steal, but the information stored on them can still be taken if accessed. Lock your desktop with a strong password that is easy to remember.
USBs	•USBs are capable of transmitting viruses to computers when they are plugged in. Make sure that any found USBs are given directly to your IT department.
Digital Files	•Files on both computers and USBs can be stolen. Encryption – a method of encoding stored information – is a powerful technique for protecting important information on these devices.
Passwords	•Many people allow their computer to autofill account user name and password information. Be careful when using this feature; if somebody steals your device, they too will be able to access your accounts.

What Could Happen?

Computer Security Scenario

Imagine a situation in which an employee named Rob is forced to leave his laptop alone on his desk. A passing colleague, Molly, notices that Rob forgot to close and lock his computer before leaving. Sitting down, Molly opens Rob's internet browser and visits a common email website. She notices that Rob has allowed his email account credentials to be filled in automatically.

Molly now has access to Rob's email account. If she wished to do Rob harm, she would be able to use this new access to:

- Change the password to Rob's email so that she can use it later to do more damage.
- Change the passwords to any other accounts that Rob has linked to this email account by using it as a user name.
- Erase all of Rob's emails.
- Send harmful emails to Rob's friends, family, and colleagues.
- Discover Rob's personal information by reading his emails.

This scenario demonstrates the importance of ensuring that corporate and personal devices remain protected, even when you are not using them.

Physical Computer Security Requirements

We require that you:

- Must password protect your university devices
- Must keep your password secret
- We require you log-off or lock your computer when leaving your desk
- Must not access critical corporate information from personal devices

An Attacker's Common Practices

When you enter passwords into your computer, you are not invisible. Somebody wishing to access your computer in the future may try to discover your password by watching you type it into your computer.
Always be cautious when typing your password into your device, especially when you're around other people.

Even the strongest passwords can be stolen when hackers target the user.
Somebody that wants to access your computer may attempt to trick you into giving them your password. They can do this by asking you in person or by sending you a phishing email.
Never share your password with anybody, no matter how much you trust them.

Using the same password for every account is like creating a master key.
If somebody is able to determine this master key password, they will be able to access all accounts that use this password, provided they know the user name that goes along with it.
Use different passwords for each account you create.

Be Proactive

There are many things that you can do to help keep your devices safe while you are not using them:

- ✓ If available, use cable locks to secure your laptop when you are away from your desk. This will help prevent someone from stealing your device.
- ✓ Lock all devices with strong, unique passwords. This will help prevent someone from stealing your information.
- ✓ Do not share your passwords with anybody, even people you trust.
- ✓ Only insert USBs into your computer if you trust that they will be free of malware. If you are unsure, deliver the device to your IT department.
- ✓ Don’t allow files that contain critical corporate information to be easily accessible.
- ✓ Avoid allowing your browsers to automatically fill in your credentials when logging into accounts. While this may be more convenient, it puts you at risk.

Reporting and Contact Information

If you have any general questions:

- Bruin Support Services at 1.800.756.7920

A private, non-profit institution founded in 1966, Bellevue University is accredited by the Higher Learning Commission through the U.S. Department of Education. For general information, please call 1.800.756.7920.