How to handle a suspected security incident

A cyber incident can happen to anyone - a click on a fraudulent email, a lost laptop, an unknown application that installed itself...
The important thing is not to panic, but to act sensibly and in time.

What is a security incident?

We consider any event that may compromise the security of your account, device or university data to be a security incident.

Examples
- loss or theft of equipment (laptop, mobile, USB drive),
- suspicious email or message that looks like communication from CU,
- discovering that you have logged in to a fake CAS website,
- unusual behavior of the computer (sends emails by itself, slows down, opens ads),
- sudden lock of files with ransom demand,
- suspicion that someone else is using your account.

What to do immediately?

The procedure can vary according to the type of problem – it is not always necessary to do all the steps right away.

If you have received a suspicious email or message
- do not click on links and do not open attachments,
- forward the email to IT support or the security team for review.

If you suspect that a device is being attacked or lost
- if the IT support does not say otherwise, **disconnect the device from internet** (Wi-Fi, cable)
- don't try to solve the problem yourself or install "cleaning" tools
- leave the device off or offline according to the IT support instructions.

Change your CAS password
Change your CAS password especially if:
- you have logged on to suspicious or fake sites,
- you suspect that your account is being misused.

Use another, trusted computer and choose a new, strong password that you don't use elsewhere.
Report the incident to faculty IT support or the CSIRT-CUNI security team
- the sooner you report the incident , the easier it is to limit the damage.
- if you're not sure if it's an incident, **you should better consult** – even suspicion is important.

Don't investigate the problem yourself
- don't install any "cleaning tools" or download suspicious software
- leave your device off or offline until an IT worker has checked it.

How to report the incident?
Provide as much information as possible when reporting – this will help resolve it quicker.
For detailed procedure, see the Security Incident Reporting section , where you will learn how to describe the incident, who to send it to and how the solution is progressing.
If a device with personal data of students or employees is lost, the IT department will further report the situation to the **Data Protection Authority**, as required by legislation.

How do you know if it was an incident?
You **can't suddenly log into** your university account.
Your **password has changed** without your knowledge.
Messages **that you didn't write are being sent** from your email.
Files have a missing extension or can't be opened.

A **ransom note or a "virus" alert** will appear on the screen.
You better **act now** – even a false alarm is better than an overlooked attack.

How to prevent incidents
Be careful when handling emails and attachments.
Do not install software from unknown sources.
Use strong passwords and two-factor authentication.
Back up important data regularly.
Update your system and applications regularly.

Frequently Asked Questions (FAQ)
Should I report an email that "just" looked suspicious?
- Yes. Even if you haven't clicked on anything, it will help the IT department detect ongoing attacks and protect others.

I clicked on the link, but didn't enter a password - should I do something?
- Report the incident, just to be sure. Attackers can collect data or IP address information without entering a password.

Do I have to report the loss of a laptop with an encrypted disk?
- Yes. Although sensitive data cannot be leaked due to disk encryption, the university must keep track of such events, according to the GDPR.

How to proceed when an attack is suspected in 5 points
3. Change your CAS password from another, trusted device.

1. Stay calm.
4. Report the incident to IT support.

2. Disconnect your device from internet (Wi-Fi, cable, cloud sync).
5. Don't try to solve the problem yourself. Wait for the IT department's instructions.

Remember *: Quick response can protect not only you, but also university systems and your colleagues' data.*