How to detect a data breach - instructions for every user

Symptoms of a data breach

1. Your user accounts are locked.
2. You get an email notification about somebody logging into your account.
3. You get suspicious emails from your colleagues.
4. Your email outbox contains odd emails.
5. Your computer is unusually slow.
6. Files appear or disappear.
7. Antivirus alerts on your computer.

If you notice these symptoms or other suspicious activity, contact your organization's IT security.

If you suspect a data breach:

If you suspect a data breach, here are the steps you should do in a nutshell:

1. Do not panic.

Start keeping record of your actions. This ensures that in later stage you can differentiate your actions from the perpetrator's actions.

2. Do not shut down potentially compromised computers

Do not shut down potentially compromised computers and try to avoid using them if possible. Do not run antivirus checks or similar.

3. If necessary (cryptomalware, active data leakage or similar cases), disconnect potentially compromised computers from the network, or isolate them from rest of the environment using firewall.

Before disconnecting systems from network make sure what effects there might be. Damages from uncontrolled shutdown might be more severe than damages from the original compromise.

4. Collect all background information about the incident and potentially compromised computers.

- What happened, where and when?
- What is the role of the computers?
- Who owns the computers and can make decision regarding them (i.e. shut down a service)

5. Contact your organization's information security team or call Nixu directly +358 40 821 6432.

If you are Nixu CSIRT customer, please use your organization's dedicated number.