Published on *University of Colorado* (https://www.cu.edu)

Incident Behavior [1]

Incident Behavi

John sat staring at his TV screen blown away b
just watched. The words of the agent still runn
his head: FBI, breach, hundreds of thousands o
He remembered the scene in which the victim
acting out of the norm, when the victim's mou
its own. The actor dismissed that as being para
third espresso of the morning. Anyone, howev
was not going to end well.

Hopefully this scenario never becomes your re
to do and who to talk to if your computer gets
important to know what your responsibilities a
Fortunately John remembered the following s
peculiar behavior on his computer:

- Stop all work and do not use your compute
- Call your campus IT Security Office or Help
  instructions.
- Inform the representative of all you can rec
- Inform the representative of the nature of
  data that is considered confidential or high
  data that is subject to compliance requiren

Overview

We know you are concerned about protecting your computer and information and take steps to secure them. However— just like driving a car —no matter how safely you drive, sooner or later you may have an incident. On this page we will teach you indicators of behavior that can be considered incidents, and if so what you can do about it. Ultimately, the quicker you detect computer anomalies and the faster you respond, the better you can mitigate any harm to you or your organization.

Incident behaviors

First, you need to understand that in many cases there is no single item or step. Instead there are usually several indicators. If you identify a combination of these, this implies your computer may be under attack. Here are some examples.

- Your anti-virus program has triggered an alert that your computer is infected, particularly if it says that it was unable to remove or quarantine the affected files.
- Your browser's homepage has unexpectedly changed or your browser is taking you to websites that you did not want to go to.
- There are new accounts on your computer that you did not create.
- There are new programs running that you did not install.
- Your computer is continually crashing or running very slow.
- A program on your computer requests your authorization to make changes to your system, although you're not actively installing or updating any of your applications.
- Your firewall alerts you that a program you do not recognize is requesting permission to access the internet.
- Your mouse or cursor seem to move on their own as if they are being controlled by someone else.

How to Respond

If you believe your computer is being targeted, the sooner you respond, the better. If the computer you are using was provided to you by your employer or is used for work, do not try to fix your computer yourself and do not turn the computer off. Not only you may cause more harm than good, but you could destroy valuable evidence that can be used for an investigation. Instead, follow these steps:

- Stop all work and do not use your computer until advised otherwise.
- Call your campus IT Security Office or Help Desk and follow their instructions.
- Inform the representative of all you can recall.
- Inform the representative of the nature of your work and if you access data that is considered confidential or highly confidential, or if you access data that is subject to compliance requirements.
- If for some reason you cannot contact your organization, or you are concerned about a delay, disconnect your computer from the network and then put it in sleep, suspend or hibernation mode.

Even if you are not sure you have been targeted, it is far better to report now just in case. Your campus has processes and a team in place to handle situations like this, let them handle it. Please also do this if you use your personal computer to perform your work duties.

These steps may seem trivial, but each step is important to quickly and accurately determine the nature of the behavior and the impact on you, your campus, and the university as a whole.

This months content adapted from SANS OUCH newsletter located here: https://www.sans.org/security-awareness-training/ouch-newsletter

[2]

Need Help?

UCCS Help Desk [3]	CU Denver & Anschutz Help Desk [4]	CU Boulder Help Desk [5]	CU Information Systems Help Desk [6]
719.225.3532 [7]	303.724.4357 [7]	303.735.4357 [7]	303.860.4357
helpdesk@uccs.edu [8]	UCD-ITS-HELPDESK@ucdenver.edu [9]	help@colorado.edu [10]	help@cu.edu [11]

Source URL:https://www.cu.edu/incident-behavior

Links
[1] https://www.cu.edu/incident-behavior [2] https://www.sans.org/security-awareness-training/ouch-newsletter [3] http://www.uccs.edu/helpdesk/contact-us.html [4] https://www1.ucdenver.edu/offices/office-of-information-technology/ [5] https://www.cu.edu/www.colorado.edu/oit/support-training/it-service-center [6] https://www.cu.edu/uis/uis-service-desk/uis-service-desk [7] https://www.cu.edu/
[8] mailto:helpdesk@uccs.edu [9] mailto:UCD-ITS-HELPDESK@ucdenver.edu [10] mailto:help@colorado.edu [11] mailto:help@cu.edu