Information Systems and Services (ISS)
Compromised PC FAQ

Information Systems and Services
College of Health and Human Development

A compromised computer (PC) is a computer that has a virus, Trojan or other malevolent program installed. Compromises can occur when the user opens unsafe/unknown attachments, visits web pages that are infected or bogus, or clicks on bad links in emails. In these cases the PC must be rebuilt to clean the infection. A simple compromised PC can be repaired within a day or two.

On the other hand, if PII data (Personally Identifiable Information- SSNs, credit card accounts, bank accounts, driver's license numbers) is discovered on the compromised PC, further action must be taken before the PC can be rebuilt and returned to the user. ISS is required to alert the PSU Security Operations & Services (SOS) office. Once that occurs ISS is not involved in the case until SOS has provided ISS with an update and a course of action. The course of action can be as simple as rebuilding the PC and returning it to the user, or as complex as requiring an outside firm to do forensic analysis of the hard drive and/or an outside firm being contracted to contact all people whose PII was found on the system. **Before the user can get back their PC and any files from the hard drive, this process must run its course.** We have seen up to a **two month** delay before the user gets back their PC.

Here is a short summary of the steps involved in a compromised situation:

- ISS is notified by SOS that a PC is compromised
- ISS must remove the PC from the network ASAP
- ISS will check Identity Finder logs and/or perform an IDF scan to look for PII
- ISS will notify SOS and the user of the scan results
- If there is over 500 instances of PII on the PC ISS turns the hard drive over to SOS for further analysis. We then wait to hear what the next step is.
- If no PII was found the system can be rebuilt and returned to the user
- If PII was found, an outside firm may be employed to do forensic analysis of the drive. SOS may also require the College to notify all parties whose PII was on the drive of the incident. Both of those efforts entail costs – sometimes high costs. A recent compromise involving 1800+ PII instances approached $5000. That cost is the responsibility of the unit where the user's home appointment is.

In an attempt to answers other questions you may have on this process, here is a short FAQ:

My PC is gone, where did it go?
The computer was removed by ISS because we received a compromised computer notice from SOS (Security Operations and Services). This notice is sent to ISS when a University computer is committing malicious actions (sending out spam or acting as part of a network of compromised computers are a few examples). We strive to alert the user and/or a representative in the area ASAP that the PC must not be used and will be taken for analysis.

Can I copy files from the compromised computer before it is taken. I'm working on something really important?
Unfortunately no, the PII scan relies on file access dates to identify compromised files. No changes can be made on the PC. ISS understands that you need the computer and data to perform the duties of your job and that you have deadlines. **That is why we strongly encourage your use of the PASS system, and also why the College covers the cost of PASS for you. You can continue working uninterrupted by making use of your PASS files while the compromised PC is being evaluated and rebuilt.** Please visit this link (http://www.hhd.psu.edu/iss/training/training.html#pass) for information on how to obtain PASS space.

Where was the compromised computer taken?
It was brought to the ISS offices in the BBH Building so that we could begin the analysis.

When will I be able to access my files?
We can't say until a PII scan is run on the PC or a check of the logs for Identity Finder show that a recent scan took place. If PII is found we must notify SOS and turn the hard drive over to them. They then dictate the schedule. The drive can be with SOS anywhere from a few weeks to a few months. We have seen the process take up to 2 months. Once SOS completes their work we will get the drive back, rebuild the PC, and return it to the user sans the PII.

What can I do to prevent a compromise from occurring again?
As always practice safe computing. Do not open attachments that you are not expecting, do not click on email links without checking to make sure they are valid, only install software that is directly related to the work you are doing, and do not click on popup ads. Run your own Identity Finder scan (for more info contact ISS or attend our training class on IDF). Delete or move to alternate storage media all social security numbers, bank account information, driver's license numbers and credit card information. Removing this data from the computer makes certain that it cannot be misused by hackers. **Keep a backup of your files on PASS, in the cloud, or on external devices like USB flash drives.** That way you can continue working with a loaner PC that we can provide for you.

How do I get more information on this situation?
We will let you know if we found PII on the drive. We will try to inform you of SOS's progress during the SOS phase but we aren't always notified as they do their job. You can call ISS to obtain an update.