www.intrepidnetcomputing.com

B. Kirkpatrick, Ph.D.
Security Consultant

Phone: 1-406-988-0179
Cell: 1-406-660-7100
bbkirk@intrepidnetcomputing.com

February 28, 2016

Computer User

RE: How to Identify Hacking

Dear Computer User,

Access to secure computing is mediated in part by the user's ability to detect security breaches. To date, there is no reliable automatic way to detect a broad range of breaches. Therefore, the user's ability to detect breaches and hacking is the main barrier to achieving secure computing.

Intrepid Net Computing defines computer security as a state of network and operating systems that allows deterministic, or predictable, execution of computer programs. This determinism is defined with respect to a closed system of hardware and software, and it allows for bugs in the execution of both the operating systems and network infrastructure. Indeed, determinism means that buggy behavior is repeatable and predictable.

Intrepid's working security hypothesis is that there are few sources of non-determinism in computing and that hacking is the most common source. Indeed, Dr. Kirkpatrick believes that with a little education people can learn to detect both the signs of non-determinism and the signs of hacking. The sources of non-determinism are ranked for their frequency of occurrence with the most frequent at the top:

1. user behavior,
2. hacking,
3. parallel-computing faults due to race conditions, and
4. hardware failures.

If you are the only user of your computer and all of your updates are manual, then your computer should usually behave very predictably to you. This is because parallel-computing faults and hardware failures are rare events. This means that you should be able to distinguish security breaches from normal computer behavior. Intrepid aims to educate its clients about how to distinguish the signs of hacking from the signs of other faults and failures.

There are many signs of hacking. This is not an exhaustive list, so please contact Dr. Kirkpatrick to trouble-shoot other suspected security breaches. The list is as follows:

1. fraud or identity theft
2. unauthorized changes in an online profile, such as your Facebook page
3. file loss
4. data loss, such as loss of calendar data
5. loss of passwords stored in an electronic key chain

6. loss of access to a disk or a disk partition, particularly an encrypted disk
7. keyboard faults
8. broken software components that previously worked, particularly if the primary user did not update the system
9. changes to documents that were not introduced by the document owners
10. software errors that appear suddenly when the software was not updated
11. people knowing things about you that you thought were confidential

Many of these signs of hacking inspire users to seek IT help where the IT professionals fix the symptoms of the hacking without addressing the underlying cause. In order to have secure computing, users need access to security-aware IT which will help triage security breaches from normal IT problems. Intrepid Net Computing can help with this triage and help clients learn the fundamental signs of security breaches. Please contact Dr. Kirkpatrick if you believe you had a security breach.

Please keep in mind that your hacker benefits from hiding the signs of their security breaches. A hacker gets the most mileage out of hacking when they lurk on your computer and quietly gather financial data, insurance data, medical data, industrial secrets, or other valuable information. Some hackers may be interested in harassment or ransom schemes, and they may disable your computer or your access to your own information.

Sincerely,

B. Kirkpatrick, Ph.D.
Security Consultant