BCSI Investigations

July 2014
Volume No. 6
Issue No. 12

THE INVESTIGATOR

In This Issue

About Us

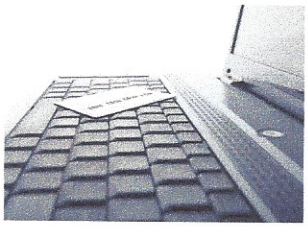
Since 2000 BCSI has performed hundreds of successful investigations.

Our integrated team of investigators and support services ensure that the investigations are conducted in a timely fashion with leading edge techniques.

BCSI is considered the platinum standard of the industry based on the quality and the wide spectrum of its services as well as the expertise of the investigators.

Quick Links

Phishing



Requests for your account information otherwise known as "phishing scams" are becoming increasingly more popular among criminals. Phishing emails often look genuine and in fact, they often copy an institution's logo and/or message format. The email links will have a URL address that is similar to, but not the same as a financial institution's site.

Here are some warning signs that you should look out for:

- The email does not address you by your proper name.
- The email may have spelling or grammar mistakes.
- The email may state that your details are needed for a security and maintenance upgrade, to "verify" your account.

Computer Hacking

Criminals are now using old fashioned technology to hack into people's computers. A criminal calls you on the phone while posing as a computer technician from a big company such as Microsoft, and claims they have detected a virus on your computer. They then ask for remote access to your computer so they can fix the problem.

Social Media

Don't rely on any phone number or website the caller provides as it may be fake. Instead, you should do your own research. Search for a published help line for your hardware or software manufacturer and dial it yourself.

Pharming Scams

Pharming scams (also referred to as page-hijacking) are when you are redirected to a fake version of a website which may look identical to the website you were trying to view. In this scam, the legitimate URL you typed into your web browser automatically changes and redirects you to a fake address.

There are two methods of pharming scams which both lead to potential identity fraud. The first method is when the victim's computer is infected with a virus which then causes changes on the computer which redirects you to the fake site, even if you type in the correct web address. This method of pharming may be identified by some antivirus software programs. The second method is more sophisticated and undetectable by antivirus programs making it harder to protect yourself. In this case, an external server is attacked resulting in you being redirected to a fake website unknowingly. As your computer is not infected, your antivirus software cannot help you.

Here are some warning signs that you should look out for:

- The pharming website will often have a strong resemblance to a legitimate website, however the web address will be slightly fake.
- The pharming website may ask you for personal information whereas the original site didn't. E.g. an online banking website generally asks for your username and password but a pharming website may ask for your bank account or credit card number as well.

Phoney Fraud Alerts

A phoney fraud alert is similar to a phishing scam and can come in the form of an email or a phone call claiming to be from your financial institution. The scammer

tends to tell people that their credit card or account has been cancelled due to criminal activity or because they suspect your card or information has been stolen. This is a trick to get you to tell the scammer your account information. You will be told that a suspicious transaction has occurred on your account, perhaps a large purchase or a purchase in a foreign country.

Here are some warning signs that you should look out for:

- You receive an email or call from someone claiming to be from your financial institution asking about recent activity on your credit card or bank account.
- You are asked to confirm your account details over the phone or by visiting a website.
- The caller or the email claims that there has been fraudulent activity found on your account or that your account has been cancelled.
- You are discouraged from contacting your financial institution.

Enforcement

The legal system has not kept up with crime. Criminals use false identities online but their footprints (i.e. IP address) remain. The Internet Protocol Address (IP address) unique to each computer can often help locate criminals operating online. Meanwhile in most cases it is necessary to obtain a court judgement or search warrant to access the registry.