IDENTITY THEFT, TAX FRAUD, MEDICARE FRAUD, CREDIT CARD FRAUD, CHILD PORNOGRAPHY AND THE DARK WEB -

THE ADVANCEMENT OF CYBER CRIMES

Marcia Shein from the Law Firm of Shein & Brandenburg

Cyber crime is here to stay and getting even more complicated as the future advances web technology and our dependency on the use of computers personally and internationally. From security breaches to sensitive government secrets and documents more and more people and countries are waging war over the internet. Here, Lawyer Monthly benefits from an exclusive article from Marcia Shein from the Law Firm of Shein & Brandenburg.

www.lawyer-monthly.com
There is not one simple category of cyber crime more prevalent than another as it is all going on simultaneously due to the ease of access to the web. Child pornography crimes are easy to commit online in the sharing and distribution of child pornography. Catching these individuals requires law enforcement phishing on dark web sites that encourage fantasy chats and exchange of pictures, identify theft and tax fraud and credit card fraud are also becoming regular events in cyber space.

There are numerous schemes for cyber fraud activity. For one example, foreigners seeking student visas are being recruited to come to the United States and apply for university entry but never show up for class instead working for a group who has stolen personal information from Americans to file false tax claims or stolen and false credit cards before anyone knows it happened. The cards are used, the false tax claims are filed and the money is deposited into student bank accounts only to send the money out of the country for a fee before anyone detects the conduct. There are numerous cyber crimes, too many to be mentioned here. Suffice it to say that social security numbers and the personal information breaches you hear about in the news are not without long term consequences to the victims whether it is the government personnel, corporations or the average citizen.

The United States needs to become vigilant in its own efforts to protect its citizens and develop a hacking army of its own not only to stop the attacks but to hack the hackers to recover the information hoping it does not get sent out in mass to others. For some reason it is easy to file multiple fraudulent tax returns without the IRS catching on that most are going to one or two people that do not match the location of the real person.

It is not easy to catch these offenders before they have gotten away with large sums of money mostly sent out of the country. By the time the government actually finds and arrests the offenders they have already caused serious losses to the individual and government.

Our firm represents federal cases including white collar offenders and cyber crimes. Corporations need to be more vigilant in protecting their information and secrets if they hope to minimize the damages being caused by hacking and cyber crime in general. Some corporations are engaging in developing their own cyber security force to try and keep ahead of the would be hackers as well as securing their operating systems and how people access sensitive information. It is however a never ending battle. A great deal of cyber crime goes unreported when the value of reporting it is low. That is why more people are using such things as Life Lock and other internet identity protection tools.

There is never going to be a 100% solution to hacking or the commission of cyber crimes and their results but there is much more that can and should be done including getting the government to update the country’s computer systems and engaging a protection and cyber attack intervention force.

The other layer of cyber crime that is getting some attention but still not enough is the dark web. It sounds sinister and it is. According to Wikipedia, the dark web is the World Wide Web content that exists on darknets, overlay networks which use only certain networks which use the public internet but which require specific software, configurations or authorization to access. The dark web forms a small part of the deep web, the part of the Web not indexed by search engines, although the term “deep web” is confusingly used to refer specifically to the dark web.

The darknets which constitute the dark web include small, friend-to-friend, peer-to-peer networks, as well as large, popular networks like Freenet, I2P, and Tor, operated by public organizations and individuals. Users of the dark web refer to the regular web as the Cleanet due to its unencrypted nature. The Tor dark web may be referred to as Onionland, a reference to the network’s name as “the onion router.” Staying up to date on these issues and problems isn’t easy and that is why cyber protection services and task forces are going to become the norm for the government, corporations and the general public.

What happens to a person who commits a cyber crime? Clearly cyber crime was going on years ago when the “Napster” developed a peer to peer file sharing program that allowed people to download and share music for free. This might have been the first significant step towards predicting the future of cyber crime. Others followed before the criminal justice system got involved. There are people who have hacked Apps that cost money, writing code to crack the App and then turn around and share the cracked Apps with others to be downloaded for free from a server in the Netherlands or some other country making it hard to stop and prosecute. There are still online programs that give Apps and music away for free when fees and royalties are required. Once someone gets shut down another shop opens up.

When representing cyber crime offenders our job is to guide them through the criminal prosecution by being vigilant in making sure the government is not trampling on Fourth Amendment rights related to searching and seizing computers, laptops and cell phones. The Supreme Court recently determined that a warrant must issue for the search of private cell phones based partly on the fact that more and more personal information is being stored on them. There are defenses for charged offenders such as having experts check to see if the computer information that is being used to prosecute the offender is in fact on the computer seized and implicates criminal activity.

There is also the issue of whether the person being charged is the actual perpetrator of the fraud or an arm of a greater conspiracy. What role did they play and did they profit from the cyber crime activity they were alleged to have participated in. Experts in the field of cyber crime forensics are often used in cases where the content of a computer is competed to see if something can be salvaged that would support a person’s innocence or lesser liability. In Child Pornography cases computer experts can ascertain if the pornography was deliberately downloaded, how often and if it was actually distributed or if the computer was accessed by someone or something else. Though this does not happen often it is important that every aspect of an offender’s case be analyzed including computer use and content.

There are so many cyber crime problems and issues facing our nation and corporations that new efforts to minimize the damages need to be a priority. If a person is accused of a crime involving the web our firm can minimize the effects through negotiations, trial or appeal. Right now we are appealing an issue dealing with web “private clubs” (not open to the public accept through private invitation), and whether a member can be charged with the same offense as the operator and monitors of the club whose conduct is both legal and illegal. For example as a member of the club you can only access adult pornography but if you are a member and get a special referral from another member you can access child pornography, is just being a member of the club with or without access to the illegal child pornography enough to be charged with and convicted of the cyber crime of possession and/or distribution of child pornography?

There is so much more to this subject but hopefully this information will get someone’s attention if not at the prevention level then at least on the representation level if accused or charged with a cyber crime.

LM

Contact:
Marcia G. Shein
Law Firm of Shein & Brandenburg
Federal Criminal Law Center
2392 North Decatur Road, Decatur, GA 30033
Tel: 404-633-3797
Web: www.federalcriminallawcenter.com

www.lawyer-monthly.com