The History of Cyber Security by Eccuni

Article published on December 19th 2011 | Internet

The term cyber crime is all the same as any other kind of crime - there is a culprit and also a victim. For the cyber crime to become successful, it needs the same component of other crime; the motive, the opportunity and the means. When one can view the brief history of cyber crime we could see that the elements for the motive, opportunity and means are few, thus computer crime is less prevalent. Indeed, profit is one of the reasons, but there are some reasons like revenge for cyber crimes like DDoS attacks as well as ego in creating malicious viruses.

However, as the accessibility and connectivity has increased, the means and the opportunity have also increased. Back then, only a few people know how to use computers and there is no reason in assaulting them; the companies during those times weren't even connected online. Since the internet nowadays is almost everywhere, the means and the opportunity has greatly increased. Now, anyone can use a computer and there are many ways to use them like networking, online gaming, and banking and money transactions

When we look back, cyber criminals were almost always more sophisticated than those individuals who are trying to deter them. And even if companies have IT security, there are only few security professionals and ms information security graduates and much fewer security tools available against threats. Today the story is almost the same, criminals may have grown more dangerous and has many ways to accomplish their dark deeds, but for some reasons the threats they pose have been greatly reduced, compared to as before.

The vulnerability in cyberspace has been greatly reduced thanks to the increased numbers of security professionals and graduates of master's degree in information security as well as many products and methods that can be used to mitigate threats. All of these can provide better security in the cyberspace for companies.

Another possible reason would be is that the laws against cyber crime have also changed; more cyber criminals are being brought to justice. Cyber crime is treated the same as any crime, any culprits caught are punished and are locked in behind bars. However, there are some skilled criminals who can escape justice from both worlds â€“ the virtual and physical world.

Even if companies will muster all their resources just provide the best IT security by hiring security experts and employing the use of technologies and best methods; the threat of cyber crime is still present. If the criminals are barred in one way, they will still seek other ways of entry. In the past, cyber criminals grew tired of directly attacking hosts and networks, they shifted their attention into other ways like attacking the more vulnerable applications. If the application is blocked, then attackers would target the end users of those companies via phishing, XSS or other attacks targeting the clients. They become the most suitable target because they are unaware of IT security and on how to keep every transaction safe and secure.

Any financial institution with weak IT security will fall prey to cyber criminals in just a matter of seconds, but banks with advanced security will be much more difficult to confront. But that doesn't stop criminals; they could easily trick the clients and steal their credentials and important information needed for banking transactions. Often times, attackers would send Emails masking as security mails asking to verify important data; once the clients make the mistake of supplying the information then his account will be compromised. Employees of companies can also fall victim to the same

method. Emails, phone inquiries and other techniques are used just to get the necessary data that can be used to penetrate the systems of the company. We can simply put it this way; the surest way to go through security is have someone else's login ID as well as password.

Sometimes, the most common reason why individuals fall prey to these vile criminals is their ignorance. Some of these individuals are still making use of computers with ancient operating systems which are more prone to cyber attacks. They didn't know that computers are not like appliances and that they needed to be updated from time to time.

The ware against cyber crime is still not won. And each side is getting better and better as years go by. Many security experts and master's degree information security graduates would agree with this statement, "It is much better to protect the individuals and company's information network rather being the cause of their downfall."

Article Source:
http://www.articleside.com/internet-articles/the-history-of-cyber-security.htm - Article Side

Eccuni - About Author:
EC-Council University is a licensed university that offers degrees and master's degrees on Security Science online. The degrees are recognized worldwide and may be used in any employment worldwide as well as the graduate certificates that they offer. With excellence and dedication as the core values, many professionals and degree holders have benefitted from undergoing the programs in this university.

More information about master's degrees in information security available at www.eccuni.us, a ms information security, a master's degree in information security, a master's degree information security

Article Keywords:
Cyber Security, ms information security, masters degree in information security, masters degree information security, Cyber crime, victim, DDoS attacks, malicious virus, networking, online gaming, money transactions, IT security, security professionals, c

You can find more free articles on Article Side. Sign up today and share your knowledge to the community! It is completely FREE!