Article Side

Look out for Safety Symbols Before Clicking the Submit Button by Mark D

Article published on December 26th 2011 | Internet

Securing our business information has become imperative these days just like protecting our physical belongings from burglars. A policeman, a security personal or even a automated surveillance device like ADT Home Security can help you in the process of protecting your home from "Door Break" events, but are you aware that business information hijack on the internet can create potential damages similar to the one caused from a burglar visit? Information theft is a type of computer security risk and it is defined as stealing an individual's personal or confidential information. Business or home users are both at risk of information theft. One example is a malicious individual stealing credit cards so they can make unauthorized purchases on another person's account. If information is transmitted over a network then it has a very high chance for malicious users to intercept the information. Every computer in the path of your data can see what you send, and they can also see what you send.

A lot of companies try to stop information from being stolen by applying some user identification and authentication controls. These constraints are best for protecting computers in a company's premise. However, to protect information on the Internet and on networks, companies use a handful of encryption methods. This is a process of converting data into an unreadable format which requires a unique encryption key to decode or decipher the actual data. There are many types of encryption or algorithm methods to make you data secured from human eyes since you will be using more than one of these techniques. Some business use available encryption software, while others develop their own.

When users send information online through an email or a web form, they will never know who might intercept it, or to whom it could possibly be forwarded to. That is why it is not a good idea to send confidential information online without properly protecting it. However, an individual can help protect their information themselves by encrypting the data, or by signing it digitally. There are so many freeware tools out there in internet with good ratings to help you in encrypting your information or to digitally sign it. Please note that these applications are not free for those who intend to use it for commercial purposes like encrypting e-books or applications that are sold online. The main purpose behind using digital signatures is to make sure that it is not a deceiver who is participating in the transaction on the other side. So, digital signatures help narrow down e-mail scams and it can also ensure that contents of a message have not been changed.

Further when it comes to browser based encryption, most of the browsers come with a basic encryption level of 40-bit. There are some upgraded or advanced browsers offers up to 128-bit encryption which indeed delivers high security since the encryption key is longer. Mostly, the encryption keys are assigned and stored in a non-reversible format like MD5 Hash which makes it difficult even for the data owner to recover or reverse the key. A website that successfully uses encrypted transactions to secure the data transmitted from the user's computer to the server is known as Secure Site. Hope you remember the padlock sign on the browser while you visit online banking sites or web forms that asks for your financial information, that symbol confirms that the site uses digital certificate with security protocol. The two most popular security protocols are Secured Sockets Layer (SSL) and Secure HTTP (S-HTTP). A digital certificate on the other hand can give peace of mind to the user since his or her information cannot be hijacked on its way to the server.

Survey reports say that 20 out of 100 people using internet are affected directly or indirectly due to identity thefts. It is an individual's responsibility to look out for all possible security methods taken by a website or email service providers before sharing his/her personal information on the internet. Please note that losses created due to identity theft may become unrecoverable since we don't

have a "Universal Law against Cyber Crime" until today.

Article Source:
http://www.articleside.com/internet-articles/look-out-for-safety-symbols-before-clicking-the-submit-button.htm - Article Side

Mark D - About Author:
Being a freelance writer and active Blogger, I like sharing my thoughts and ideas to rest of the world. I strongly feel that Identity thefts happen only when a individual's negligence in going through the security arrangements of a website before sharing his/her information. Just like the way you invest time and money in installing security devices like a ADT Home Security to protect your premises, do spend some time on security aspects before sending your valuable information on internet.

Article Keywords:
information theft, home security, adt security systems