After the hack

After the hack

> According to published reports, Visa and MasterCard recently warned card-issuing banks that a third-party payments processor suffered a security breach. This breach may have exposed the Track 1 and Track 2 data needed to counterfeit cards. The compromise, according to both KrebsonSecurity and The Wall Street Journal, happened sometime between January 21 and February 25. It's not clear if attackers had access for that entire period.

Source

Here is where the driving force is to tame the internet. To turn it into the merchant's wet dream. The idea of having a store with unlimited shelf space, without having to meet all the requirements of a brick and mortar store are strong. No having to meet safety requirements for the handicapped, no having to worry about the parking lot needing repaved and painted, no worries about collecting sales taxes in most states, no worry of fire safety inspections; just a lot of laws, requirements, licensing costs, taxes, and upkeep and maintaince go out the window with an on-line store. To be sure, there are others required in this case but no where near as many as the physical store.

In order for on-line buying to be successful, one must have total faith in the financial system to forward payment and for the store to send the goods. A break of trust in either kills the process. Here is where we run into the hacker and what it means to the customer. Today, as a credit card customer, that is not a business, your credit and charge totals are protected, provided you did your best to maintain security. Ie, you didn't just up and give out your information on purpose for fraudulent purposes. This is an attempt to keep the trust in the system going.

Every year or two it seems, we hear of a major break in, where all security is somehow bypassed, and all the protected info is stolen. Shortly after, people start seeing charges for goods they never made on their accounts. Big money is being stolen this way.

In an effort to attempt to contain the various botnets that are spamming and stealing financial personal data, the ISPs are being encouraged to fight back by a general code of conduct. You can find an earlier article here I've posted dealing with that topic. The purpose is to identify and alert computer users when their systems are infected. That too, has holes in it as John has mentioned earlier.

The on-line market place will crater with out sufficient trust in the system. Money doesn't grow on trees and these credit card companies are going to have to come up with a solution as the amount stolen continues to rise.

Share this:

- Share