

We Are All Connected

Ian Burke
11/22/2006

Computers are powerful tools and wonderful toys. We use them to balance our checkbooks, study for exams, play games, and explore our imaginations. Perhaps more than anything, computers have become a cornerstone in how we communicate. Through email, chat sessions, MySpace blogs, and the many other portals that have evolved on the Web, our options for ways to express ourselves have grown exponentially over the past ten or fifteen years. With these new avenues of expression have come new exposures, risks. Each day we tell the world a little more about ourselves; we become a little more intertwined with each other and our computers.

More and more people have credit cards today, and more of those credit cards are smart. What is a smart credit card? Technology today is storing more information, and moving more data than ever before. A credit card now comes with a computer chip which not only stores personal data about the card holder, but is able to talk to the bank and verify that that card is being used appropriately. This credit card is being recorded by your bank in their computers, on their web site, with Amazon.com or which ever web sites you do business with. With your phone company and several other utilities that you used it with as a security deposit. They have all put it into their computer systems.

So how does this really connect us? Well all of these companies have that information on their computers. A persistent hacker that is profiling you might follow that credit card. Once they get a transaction report from the bank they can presume other vendors and build a profile from there.

But isn't this information secure? Yes it is. But like every good safe, there is someone that is going to try to crack it. The most common way is with something called social profiling. The way this works is to get you to tell the attacker the information that they want. This past year AT&T had sixteen thousand account numbers stolen from an online site. The attacker then sent out what is called a phishing attack, sending emails to the account holders asking for them to go to a false web site and log into there account and reset their account information. The email contained the recipients account number so it looked authentic.

As you can see, protecting your identity is very important. The trick is to generally be cautious with what you do. Perhaps you only use computers at work. There are security guidelines to those systems. It is important that you follow them. There was a Blood-doping test lab in France that was recently compromised by an outside attacker. The attacker sent incriminating letters to other labs and news wires from the French labs computers. Now careers, people's integrity, the quality of the lab, and an entire criminal investigation that the lab was conducting are all being questioned because the security rules were not followed.

Security is never the favorite part around computers, but it can make and break a business. Here are two sides of that coin. In 2005 MasterCard International identified a third party card processor that had a security breach compromising forty million card holders. On the other side approximately fifty percent of all online orders made in the United States in a year are fraudulent. Here it pays both to ensure that the security is tight on the cardholder information and that the security around the transaction tight to prevent a fraudulent order.

So what is being done to help with all of this? California was one of the first states to introduce legislation requiring notification in the event of a breach of privacy. Other states, such as New Hampshire, have followed more recently. These laws don't simply help the consumer by ensuring that they will know if they are violated. They put pressure on the vendor to tighten security for fear of the black mark in the public eye.

Other legislation such as GLBA, HIPAA, and SOX have been past to regulate privacy and commerce. Stiffer penalties for cyber based crimes are being passed down from the courts. Recently a California man was given a fifty-one month prison sentence for selling fake drugs in an online pharmacy scheme. And, international cooperation on convicting cyber criminals is growing.

But, as we all are so aware, the issue does not stop with social engineering. What about viruses and spyware. Over the past fifteen months Microsoft has been collecting data through their "malicious-software-removal-tool" (a free utility the offer to XP/2000/2003 owners). This tool has been run approximately 2.7 times by 270 million+ unique computers, leading to the removal of 16 million instances of malicious software from 5.7 million unique Windows-based computers. In short there is a lot of malware out there and the best thing that we can do to defend ourselves is stay current with our anti-virus software. On the Brightside, a lot of this software is the same or variant of what has been. The blaster worm that was released onto the Internet several years ago is still among the top ten most removed pieces of malicious software from computers

So where do we go from here. Remember that we are all connected. We always will be. The trick is not to be afraid but rather to be safe. Pay attention to where you go when you surf the Web. Double check those emails when you get them from a bank or a vendor. Security is not a policy or a road block. When it comes to the Internet, security is your best friend.

Ref:

1. Microsoft Releases Windows Malware Stats:
http://blog.washingtonpost.com/securityfix/2006/06/microsoft_releases_malware_sta.html
2. The Executive:
http://www.hillnews.com/thehill/export/TheHill/News/TheExecutive/100506_fraud.html
3. Ecommerce – Credit Card Fraud Costs and Statistics:
<http://www.tamingthebeast.net/articles2/credit-card-fraud.htm>
4. Hackers steal data from Landis Lab: http://www.washingtonpost.com/wp-dyn/content/article/2006/11/14/AR2006111400389_pf.html