

Network Security Compromised Company Goes Bankrupt & Customers Fall Victim to Identity Theft as a Result of a Good Employee Doing His Job

Yes, you read that correctly!

This network security document shows you in detail how this type of situation CAN happen to you, if your network is not properly secured.

Situation: An employee performs a search on examplesearchengine.com to find a part needed to repair a customer's vehicle and within 12 hours, the entire company goes bankrupt in addition to having the identities of its 20738 customers stolen.

Disclaimer: While this example is not based on a specific known real life situation, this type of situation can easily occur in network environments that lack proper security. Each type of incident described in this document has occurred in the past and can easily occur again in any corporate computer environment that does not have a properly secured network computing environment. If all these elements are combined, the type of situation described in this document can easily occur.

***To view a list of US Companies, Colleges, and Universities who have enabled cyber criminals to steal their customer data by not protecting their networks and data assets in a responsible manner, visit <http://www.privacyrights.org/ar/ChronDataBreaches.htm> You may be surprised and shocked to see the US Companies, Colleges, and Organizations who have made this list.*

Example Situation (Computer User): Its 6:45pm on a Wednesday evening. Mike the parts guy is trying to get one last order finished up before heading home. He has to locate a hard to find aftermarket auto part and purchase it to fix a vehicle. So he heads off to www.examplesearchengine.com to search for 2003 Pontiac aftermarket special order part.

As he scrolls through the first page of his examplesearchengine.com search, he does not find anything so he hits the next button to more parts suppliers. He also takes notice that on each page of his browser he notices the online advertisement for Connie's Seafood Restaurant. He also takes note that when he hits next and proceeds to the next page, the advertisement has now changed to an ad for Red Dragon Whiskey.

And like a good employee, Mike the parts guy never clicks on any of the examplesearchengine.com advertisements because he is busy searching for the part needed to fix the customers car. He then continues on to the next page of the examplesearchengine.com search, and now an Old Navy advertisement appears in place of the Whiskey advertisement.

Eventually Mike finds a supplier who has the part, places the order, and leaves for the evening.

MIKE'S ACTIONS ON THE INTERNET JUST CAUSED A MASSIVE NETWORK SECURITY BREECH RESULTING IN THE COMPANY GOING BANKRUPT ALONG WITH COMPROMISING THE IDENTITIES OF ITS ENTIRE CUSTOMER BASE!

Here is How it Happened.

Example Situation (Organized Hacker): Ten days before Mike went out to conduct his parts search on examplesearchengine.com. An ex Chinese intelligence officer turned cyber criminal named Yinmin Wu with ties to the Russian mafia just had one of his cohorts bring a web server online in the You Name It Hosting and Co-Location Facility located in the Netherlands. While his server is disguised as a business server which hosts over 300 small business web sites, its main purpose is to house a directory that contains several custom virus and Trojan horse files.

Example Situation (Organized Hacker): Several days after Yinmin's server was brought online, a cyber criminal working with Yinmin Wu, named Vladimir Petrovsky, has purchased examplesearchengine.com advertising space and has created placed several advertisements on examplesearchengine.com using stolen credit cards along with a stolen laptop while connected to a local ISP via a dial up connection in a cash only hotel outside of Moscow. This kind of set-up means, he cannot be stopped before causing the damage.

While the advertisements he created and posted onto examplesearchengine.com with his newly purchased advertisement space, are for Red Dragon Whiskey, some of the source code in the advertisement references or frames in a script file that's physically located on the server that Yinmin set up several days earlier in the Netherlands.

It's important to understand that since nothing in Vladimir's advertisement, other than the html code used to create it, is physically present on examplesearchengine.com's servers, there is no way that Example Search Engine can know that any virus or hostile files are involved. It has no way to knowing that Vladimir is up to no good, because everything he uploaded to examplesearchengine.com is legitimate html advertising



code. Among the things that Vladimir's html code references or frames in to the advertisement for Red Dragon Whiskey from other servers are product brand photos, logos, and graphics, so nothing, not even the image files are physically located on examplesearchengine.com web server.

What Exactly Happened?

After Yinmin Wu and Vladimir laid the ground work, all Mike the parts guy had to do was to accidentally stumble upon the Red Dragon Whiskey banner advertisement as he was performing his daily work duties. He does not have to click it, or mouse over it, it merely has to automatically display itself like all banner advertisements do as users click through certain search engines, or web sites.

If the pc he was using did not have proper or updated antivirus or security software, or the network his pc operates in is not properly secured, the following situations can happen.

Once the banner advertisement is displayed, the script that is written into it that automatically downloads and extracts one of the virus.zip files from Yinmin's server in the Netherlands to the local pc workstation. Once extracted, the virus file begins logging all keystrokes, such as usernames, passwords, account numbers, payment information, etc. The virus file also starts performing network discovery to identify other computers or servers that may be present on the network and records that.

The recorded information is then sent to a hacker located somewhere on planet earth, but in a nation that does not have friendly relations with the United States. This makes it impossible to find and prosecute the hacker. The hacker might also be doing his job to finance a terrorist organization or foreign power that is hostile to the United States.

The hacker who receives the detailed transmission can then attempt to make purchases using any recorded account numbers or payment information. Often times many small purchases do not cause alarm. These small purchases can be made to mob owned or fly by night businesses that were purposely set up for doing such an activity.

The hacker can also execute commands through the Trojan horse file to break into the companies database and steal customer records, financial, payment, and account information including social security numbers. This information can then be sold or used to create fake identification, or commit identity theft.

This type of breach has the potential to completely wipe out a company along with all of the customers in its database provided critical identity related information is present.

If the company has no IT department or extremely lax network security, additional long terms security breaches can occur since the hackers have already gained access to the network.

Examples of such long term breaches can be

- ARP Poisoning Attack
- SQL Injection
- Cross site scripting attack
- And many others

These types of breaches can do immeasurable damage to a business and its customer base.

Details as to the specific steps that are used to facilitate these kinds of complex security breaches can be downloaded at www.aloyecomputer.com . the document is entitled "Security Breach Addendum".

Please read them and consult your technology service provider if you have questions or see something you do not quite understand.

Bottom line is that if your company does not have airtight network security, which often costs hundreds of thousands and sometimes millions of dollars, your company is at risk.

Can you afford that risk?

