

Security and Your Business



Newsletter # 4 – July, 2008

Welcome to the Archimedes Technologies, LLC Security Newsletter. As a Trend Micro Partner, Archimedes Technologies has access to analysis of the latest threats to your business. From time-to-time we will send a newsletter on security threats of concern. The purpose of our newsletter is to inform and educate you of the threats to your business.

In this edition of our newsletter we go on the trail of a typical phishing email. Then we review the Berkeley Center for Law and Technology's report, "Measuring Identity Theft at Top Banks (Version 1.0)."

Is that mail really from your bank?

Having received my third Capital One Bank Security News & Alert, I decided to take a look at where it really came from. The email below looks legitimate and the return address appears to be from Capital One, but close examination tells us that something is amiss. The link in the email starts off looking like Capital one but most normal URL's are WWW.<COMPANY_NAME>.COM/PAGE. The very long URL below leads to an infected active-x control.

Michael Keller

From: Update Department [help@capitalone.com]
Sent: Monday, July 07, 2008 6:18 AM
To: mkeller@archimedestech.com
Subject: Capital One Bank Security News & Alerts

ATTENTION TO ALL CAPITAL ONE BANK CUSTOMERS!
CRITICAL UPDATE, JULY 7TH 2008
A critical update is available to remove unacceptable symbols from the wire submission page that is included with Capital One Bank Treasury Optimizer.
Critical Updates are intended to fix potential security risks in Business Objects of Capital One Bank.
These updates are highly recommended to ensure the security of Capital One Bank products.

For additional information about the latest service pack for Windows, click the following link to view the article in the Capital One Update Base:

To Start Update Press NEXT>>
<<http://top.capitalonebank.com/pub.login.htmlbank.serv.manager.cgipage.showshow.038801311.type.activex.compri.gb5d.com/login.html>>

2008 Capital One Services, Inc.

Let's take that very long URL and see if we can find out whom it belongs to:

```
Whois Server Version 1.3
Domain names in the .com and .net domains can now be registered
with many different competing registrars. Go to http://www.internic.net
for detailed information.

No match for domain "TOP.CAPITALONEBANK.COMPUB.LOGIN.HTMLBANK.SERV.MANAGER.CGIPAGE.SHOWSHOW.038801311.TYPE.ACTIVEX.COMPRJ.GB5D.COM".
>>> Last update of whois database: Mon, 7 Jul 2008 08:17:11 UTC <<<
```

Well, that was a dead end. So we have established this is a bad email, phishing for your information, pretending to be from Capital One. Just for fun, I dug deeper to see where it really came from. This bogus phishing email originated in Turkey.

Network Contact Information: The following details refer to the network that the system is on.

 abuse@ttnet.net.tr
 +90 312 313 1949
 Turk Telekom Bilisim Aglari Dairesi Aydinlikevler 06103 ANKARA

[Click here to hide the in-depth information on this email \(more info\)](#)

- The senders IP was - 85.103.64.222
- The sender of this email appeared to have the address help@capitalone.com. This information is easily faked so should not be treated as conclusive.

SOMETIMES YOU CAN'T PROTECT YOUR IDENTITY

The first true report of how major banks protect your information

I have a personal reason for writing this article at this time. I received a very plain envelope that looked like junk mail, not something I'd rush to open. It was a form letter from BNY Mellon informing me they'd lost a backup tape in February and our Social Security numbers were on the tape. They were really sorry, but it took them from February to figure out what they lost.

I pay for a service that has my credit report handy. I requested a report from them, and there it was: a credit search by Bank One to open a new credit card in my name. I don't do business with Bank One and I didn't ask for a credit card. So how safe is your bank?

The Berkeley Center for Law and Technology recently published "[Measuring Identify Theft at Top Banks \(version 1.0\)](#)" by Chris Hoofnagle. The report can be found at <http://repositories.cdlib.org/bclt/lts/44/>. According to the report, 25 institutions account for 49.9% of identity theft. Capital One (our previous phishing email example) rates number 5 on the list of worst offenders. Please read the report, which I have attached for your convenience.

Our conclusion: Sometimes you can't protect your identity. Identity theft is a very interesting dilemma. In this case, we receive a letter telling us that our information had been exposed and says we can have a free credit report to check on that exposure. It then asks us to go on a web page and enter in all of the information we are trying to protect, to the people that just exposed our information. These agencies normally have a phone number, it may be better to consider using the phone.

There is a quick and dirty way of placing a fraud alert on your credit report for 90 days and get a free credit report. And this is the method I used. The three credit bureaus offer toll-free phone service asking for your street number, zip code and Social Security number via a touch tone phone. Call any one of the credit bureaus and they contact the other two. The numbers are below.

Fraud Alert Numbers

Equifax 888-766-0008

TransUnion 800-680-7289

Experian 888-Experian

You will receive three letters in a matter of days telling you that an alert has been placed on your credit report. The fraud alert is just a start in the many steps to protect your identity. But it is a very good first step and done early enough can save you a tremendous amount of time and trouble.

In The NEWS

New Jersey makes it tougher on businesses in State v. Shirley Reid

The decision was hailed as a victory for privacy but it just made it that much harder for businesses that allow remote access. Read the story here:

http://www.ibls.com/internet_law_news_portal_view.aspx?s=latestnews&id=2043

XP is Dead... But it's not cold yet

Microsoft announced that XP would not be sold after June 30th, 2008. What they didn't tell you is that you don't have to go Vista just yet. You can still buy XP if the manufacturer purchased their licenses prior to June 30th or if they took advantage of the little-known downgrade policy. Dell has assured us that we will be able to purchase PCs with XP Pro until at least January 31st, 2009. For an additional \$50 Dell will include Vista Ultimate disks and drivers with your XP Pro PC. This provides upgrade protection while allowing your business to operate as usual. Microsoft will support XP through April 8th, 2014 but mainstream support, meaning bug fixes, will end April 14th, 2009. Only Microsoft Enterprise Support clients will get XP support through 2014.

Windows 7 is being tested by Microsoft as the follow on to Vista. Could Vista be the next Windows ME? Businesses are not thrilled with Vista and not looking to upgrade. Perhaps Windows 7 is the fix.

However, it is known that Windows 7 is based on the Vista core. Windows 7 is expected to release in January of 2010.

Contact us

Please contact us to discuss your security requirements. We can be reached on the web at

Info@archimedestech.com or at 973-845-6027.