

I was a BONEHEAD!

Confessions of Jeff Mulligan, Internet BoneHead

As you probably know, I make my living in online. I'm a full time Internet marketer and I spend my days trying to learn as much as I can about this business. I'd like to think I know a thing or two.

Which is why I'm so furious at myself for getting scammed today. And it almost cost me over \$571 ☹

Have you heard of phishing?

This is when some spammer is sending you official-looking emails trying to get personal information such as credit card numbers, social security number, PIN numbers, etc. Then they use this information to steal money from you.

I am embarrassed to say that I fell for this low life scam.

And I'm admitting this to you as a reminder not to do the same.

Here is what the email looked like:

Subject: Activate Your BillPay



Dear Citizens Bank Customer,
We've upgraded our service so you can schedule fund transfers. And with our improved BillPay, you can now pay bills on one screen. We will require all Citizens customers to sign up for this, please fill in your card information now to avoid extra upgrade fees being withdrawn from your account later on.

*** BillPay is a free service from Citizen Bank ***

Click on the link below to activate BillPay:
<https://www.citizensbank.com/billpay/activate.asp>

[Privacy & Security](#) © 2003 Citizens Financial Group. All rights reserved. [Terms of Use](#).

It looks real enough. But as someone who builds web pages, I know that it's very easy to swipe a logo. The tricky thing they did was make that blue link look so good, when in reality it was not a text link but a graphic. That's what got me. Because I saw the citizensbank.com domain.

When I went back to look at this e-mail afterwards I realized what happened. I discovered that it wasn't a text link but a graphic link. It actually lead to an IP address. But by then I was just in a hurry to get this done and move on to real work.

When I clicked on the link, I was taken to a very official looking page where I STUPIDLY entered my account number and worst of all, my PIN number.

Here's the really tricky thing they did: They popped the real Citizens Bank website underneath their phishing form.

That was ingenious. I've got to give them credit for that bit of subterfuge.

I didn't give it a second the entire process a second thought, until my bank called tonight and asked me if I had done any unusual transactions. I said, "No, except for activating my BillPay account."

As soon as I said that, **it hit me in the stomach like a sucker punch.** I had been scammed.

Sure enough, the man on the phone informed me that someone from Sweden had sucked out more than \$500.00 from my account. In one way I was lucky. I had a lot more than that available and thanks to the antifraud systems of the bank, my loss was limited.

In fact, after filling out a few forms and an investigation, they even gave me back the money. I was lucky.

The ironic thing is that I have seen these phishing emails 100 times in my inbox. Most of the ones I have seen have been trying to get my PayPal information. I've always laughed when I saw them and deleted them thinking, "Who could ever be stupid enough to fall for this?"

Well, you're reading a report from a guy who was stupid enough to not pay attention and to fall for this. Hopefully, it will make you think twice before you respond to anything similar.

A legitimate financial institution will never ask you for your pin number or your account number via e-mail. I know this. But in my rush to get through the daily emails, I forgot it for one minute. And it almost cost me \$571.00.

Feel free to pass this report along to anyone you want. The more people who are aware of this, the better. There are no links in this report and I'm not trying to sell anything other than the concept of protecting your financial interests.

Jeff Mulligan