



Phishing Trip Part III: Liability

infectionvectors.com

March 2005

Overview

Phishing attempts and related malware are unique areas of corporate liability for companies with a web presence. If a worm infected a user's machine, installed a sentinel that waited for bank information, lifted that data and posted it to a server, many people would not think to find the bank responsible. In many cases, something just like this can happen if someone executes an email attachment (consider the Beagle-launched Tooso/Mitglieder variants from early in 2005 that did just this type of thing¹). However, following the request found in a phishing attempt gets the opposite response from the majority of bank customers. Consider the following report posted by MailFrontier²:

61% of consumers feel that if they responded to a fraudulent email that had spoofed their bank or credit card company, it is still the responsibility of the bank/credit card company to reimburse them for the money lost.

The same could be true for non-banking online businesses such as ebay. This trend adds a significant burden to Internet business, possibly making it a cost prohibitive venture. This report examines the phishing trends and how they relate to corporate liability.

Legitimate Reasons for Corporate Liability

Certainly, every online business has a requirement to protect customer information. In the US alone, numerous pieces of legislation have been passed that hold companies responsible for safeguarding consumer data. These include California's SB 1386³, HIPAA for medical establishments, and the Fair Credit Billing Act. The latter stipulates that consumer losses be limited to US \$50 if their credit card is stolen and used by criminals⁴ (as well as the Truth in Lending Act protecting all but \$50 in cases of credit card fraud). However, there are cases where the individual is required to exercise "reasonable care" when dealing with their accounts⁵. Is it possible that this will extend to Internet safety in the near future? Before examining this issue, a few areas where corporate responsibility exists (by law or by consumer demand) will be addressed. This in no way is supposed to be an authoritative legal view of liability, it is evaluated from the perspective of the MailFrontier study: what corporations will be expected to do by customers when a criminal steals from individual accounts.

First, when a business offers an online presence, there are certain safeguards that are expected by users. Most users know to look for "the little padlock" at the bottom of their

browsers when making an online purchase. A company that does not offer encrypted transactions is likely to lose out in the marketplace, seeing customers shift to businesses that do provide this measure of security. A certain measure of due diligence in securing the machines that complete the transactions is also expected. If a company's database server is compromised, it is expected that a customer is not going to be held accountable for the ensuing losses.

Any type of internal theft, those crimes that employ privileged access or information, is generally considered to be free of customer liability. This type of event was made public for a large online business when an AOL employee was charged with stealing the company's customer list in June of 2004⁶.

In addition, when the individual itself is not the target of the attack (i.e.: one's bank account number is stolen because the bank did not secure its own machines), the user is not going to accept liability. This is part of a company's due diligence in protecting customer data, something most users have come to expect.

Place or Update Credit Card on File



Dear **eBay**,

During our regulary schedule account maintenance and verification we have detected a slight error in your billing information on file with eBay. This might be due to either following reasons:

- A recent change in your personal information (i.e. change of address)
- Submiting invalid information during the initial sign up process.
- An inability to accurately verify your selected option of payment due an internal error within our processors.

Your credit card on file with eBay

Card number: XXXX-XXXX-XXXX-4322 (Not shown for security purposes)

Expiration date: 11/05

Please sign in to your eBay account and update your billing information:

<http://signin.ebay.com/eBay!SAPI.dll?SignIn&ssPageName=h:h:sin:US> >

If your account information is not update, your ability to sell or bid on eBay will become restricted.

Thank you,
eBay Billing Department

A somewhat nebulous area is where the corporation provides no warning or education to users. Virtually every bank now has a "how to avoid fraud" page, explaining how phishing works and what to watch out for when doing business online⁷. Most likely, an organization is not more liable for fraud damages without this support, but it has become part of the required site inclusions for online banking/credit companies.

Liability, in the above cases, is established for the owner of the account (where the services are provided, such as Visa or Washington Mutual), not the initial target of the email. This basically means that the group on the hook for the losses is the organization that houses the actual account. This is important to note in cases where an email arrives for a user that contains a warning about a non-existent account. For example, everyone has received at least one letter “from” a bank they do not use.



Dear Bank of Oklahoma Customer,

We recently reviewed your account, and we suspect an unauthorized ATM and/ or PIN-based point of sale transactions on your account. Protecting your account is our primary concern. Therefore, as a preventive measure we have temporary limited your access to sensitive BOK Bank features. To ensure that your account is not compromised, simply hit "CLICK ON THE REFERENCE LINK" to confirm your identity as a card member of Bank of Oklahoma.

Login to your Bank of Oklahoma Online Banking with your username and password.
Confirm your identity as a card member of Bank of Oklahoma.
View your transaction history and report suspicious activity or any unauthorized charge.*

<https://onlinebanking.bankofoklahoma.com/OnlineBanking/login.aspx>

*Please do not replay to this message. Mail sent to this address cannot be answered.

Bank of Oklahoma, N.A. Member FDIC.  Equal Housing Lender
Copyright © 2005 Bank of Oklahoma, N.A. All rights reserved.

MMSULYBEYFHFWTYXWDNFTQEXUHSSWMXIHPSBOYJ

If the “request for update” or “security warning” asks for a credit card number, bank account information, and personal data, when that information is used for fraudulent purposes, the institution holding the account, not the forged “From” field will be accountable. If someone steals a Visa account number, in all likelihood Visa is ultimately going to be writing down a loss to fraud, no matter how that account number is obtained.

User Error and Fraud

All of the corporate liability discussion aside, bad judgment is the cause for most phishing-related losses. Although it is difficult to expect that every email user is aware of all the technical tricks of a scammer, it is still the trust placed in a con artist that leads to the theft. This is exemplified by cases where the user takes responsibility for the fund transfer, such as depositing a check. The Nigerian Counterfeit Check Fraud scam has burned quite a few people, who accept the implied bank contract of taking responsibility for everything that is deposited into an account.

To be profitable, the con needs to be carefully researched and targeted, requiring a moderate level of skill, or done in great volume. In the non-computer world, this requires some investment, stealing a card or receipt. Via the Internet, this crime is automated, it requires little investment or planning and can quickly drain millions or billions from large credit organizations.



Dear Huntington Client,


To provide our customers the most effective and secure online access to their accounts, we are continually upgrading our online services. As we add new features and enhancements to our service, there are certain browsers versions which will not support these system upgrades. As many customers already know, Microsoft Internet Explorer has significant 'holes' or vulnerabilities that virus creators can easily take advantage of .

In order to further protect your account, we have introduced some new important security standards and browsers requirements. Huntington security systems require that you test your browser now to see if meets the requirements to Huntington Online Banking.

Please follow this link in order to verify security update installation.

<https://onlinebanking.huntington.com/login.asp>

This security update will be effective immediately . In the meantime some of the Internet Banking services may not be available.

Member FDIC | Equal Housing Lender 
® and Huntington® are federally registered service marks of Huntington Bancshares Incorporated.
© 2005 Huntington Bancshares Incorporated

This is, of course, accepted by most credit organizations. Visa, for example, has instituted a “Zero Liability” program⁸, covering lost card losses. It appears to be an expected cost of business for these organizations; the question is, where is the breaking point for Internet users and online marketplaces?

It is common to receive email from a forged sender requesting bank/credit card information. In addition, users are routinely attacked with schemes of all varieties, from money laundering to sponsoring “transfers” from foreign countries (such as the Nigerian 419 Advance Fee Fraud family⁹). For these types of scams, most companies rely on law enforcement, general awareness training, and internal transaction reviews.

```
-----495553907493090
Content-Type: text/plain; charset=windows-1251
Content-Transfer-Encoding: 7bit

Hello,

we're dating agency "RusDeluxe" Group Ltd.
License number 00042247933 since 21.07.03.

Due the expansion of our organization, our agency need employees from USA for accomplishing of bank transactions.You must have an account in USA bank.
Payment will be made immediately, for every transaction (receiving and sending of money) you will get 400-1100 USD.

we have two offices:
1) 12 Pushkinskaya street, office #19.
   St. Petersburg, Russia.

2) 33 Bolshaya Nikitskaya street, office #7
   Moscow, Russia.

If you are interested in our offer,then you may to contact to our manager for other detailes by e-mail: rusdeluxe@km.ru or by ICQ# 338818190

Best regards!

-----495553907493090--
```

Many of these scams are clearly fraud attempts: they contain poor grammar, outlandish claims, or are directed at users that do not do any business with the “sender.” With others, however, it is more understandable when a target falls prey to the crime. The use of well-

constructed phony websites and real SSL certificates has already been documented. The use of “update now” and “patch attached” in mass mailer worms and scam attempts has discouraged most users from opening such messages for the fear of malware. However, if they don’t, and then unknowingly install a Trojan that steals account data – who accepts responsibility?

The most famous of malware liability cases is one from February of 2005, the case against Bank of America because of a \$90,000 transfer made from a customer’s account to a bank in Latvia¹⁰. The customer’s machine was infected with a Trojan known as coreflood, which captures keystrokes and sends them to a controller. The customer holds Bank of America responsible because the bank did not provide adequate warning for the malware being on the PC. If provider’s security must extend to every client that may connect to their servers, the ensuing costs would be astronomical. Beyond the technical fees and logistical nightmares, legal fees would crush any such business. This is another good example of the pressure being applied to web based businesses and again begs the question of where the breaking point is for the Internet.

What is Too Expensive?

CyberSource Corporation estimates that the overall revenue lost in 2004 due to online fraud was US \$2.6 billion¹¹. In addition, they note that since 2000 the overall percentage of revenue lost to fraud had been coming down, until 2004 when a slight increase was seen. CyberSource reports that most vendors (9 out of 10) believe the problem will not get better in 2005, with almost half of those surveyed saying it will get worse. Given those prospects, every web-based business should consider how to defend themselves against fraud attempts.

The challenge for web-based businesses is to find how much security consumers are willing to pay for, how much they expect from their provider, and where the whole process becomes too cumbersome (for themselves as well as customers).



We are glad to inform you, that our bank has a new security system. The new updated technology will ensure the security of your payments through our bank.

Hoping you understand that we are doing this for your own safety we suggest you to update your information, this will maintain your account updated.

[Log In](#)

The Strength To Help You Do More.

Certainly there are tools that banks and credit organizations can use to help customers with phishing attacks. Two-factor authentication has been adopted by a few organizations¹². Other options include a two-channel authentication system (such as using Internet sign-on and telephone verification). These hold the promise of reducing the value of a single password, however, they come at a cost to the provider.

Secure software clients are a possibility, at the expense of the corporation. Updates and configuration changes would have to occur through the secure client, as email would hopefully appear suspect when it shows up with a subject like: "Update required for your banking software, download here." Of course, there will be many scams directed at users such as this, and Trojans will be unwittingly installed, which a company could rightfully be concerned with generating lawsuits. Providing software and support requires that the business accept responsibility for at least a portion of the client's security, something that most businesses would probably like to avoid.

Fraud detection should also be in place, whether it is manual order review for small organizations or automated transfer audits for large banks. These processes, although capable of generating false positives, are valuable for preventing expensive refunds to customers that are victims of fraud.

Education is also still an inexpensive and good faith effort for companies looking to reduce fraud. Providing tips through the same web client customers already use to interact with their accounts allows the organization to help customers and themselves to reduce the costs of crime.

The question, "What is too expensive?" obviously has to be answered by each organization. It will be more important to identify the overall trend of Internet business, with respect to the general trust users place in web transactions. The use of email to pass information to/from customers has been corrupted by criminal elements already. Soon, the use of SSL may follow suit¹³. As technologies are considered untrustworthy, consumers may begin to feel completely incapable of securing their online transactions altogether (undoubtedly some users are there already) and abandon web commerce. This "critical mass" is the ultimate responsibility of those that are making a profit in Internet business; it is up to them to decide whether security is possible at a reasonable cost.

More information on awareness training and malware defense issues for companies of all sizes is available at <http://www.infectionvectors.com/>.

References

1. The Tooso/Mitglieder Trojans are dropped by Beagle-sent emails and updated via the Internet. For more information: http://www.infectionvectors.com/hotzone/beagle_bg.htm
2. MailFrontier Press Release, 10 November 2004: http://www.mailfrontier.com/press/press_finance.html
3. California's SB 1386 establishes strict liability for businesses operating in CA:
http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html
4. FDIC limits credit card/bank card losses
<http://www.fdic.gov/consumers/consumer/news/cnsprg98/crook.html>

Liability \$50 with credit, much more with debit
<http://www.pirg.org/consumer/credit/theft.htm#debit>
5. Reasonable care required of the consumer for banking matters:
<http://www.law.cornell.edu/ucc/4/4-406.html>
6. AOL User list stolen
"AOL customer list stolen, sold to spammer" Bob Sullivan, MSNBC, 24 June 2004.
<http://www.msnbc.msn.com/id/5279826/>
7. For example, see Visa's Email Protection Page
<http://www.international.visa.com/ps/products/protect/main.jsp>
8. Visa offers Zero Liability for Lost Cards
http://usa.visa.com/about_visa/about_visa_usa/history.html

http://usa.visa.com/personal/security/online_shopping_protection/security_tips.html
9. Nigerian 419 Scam Information/Law Enforcement
<http://www.secretservice.gov/alert419.shtml>
10. Bank of America Sued Because of Malware on Customer Machine
<http://www.financetech.com/focus/ecommerce/showArticle.jhtml?articleID=60400135>
11. "CYBS 2005 Fraud Report" CyberSource Corporation, 2005.
<http://www.cybersource.com>
12. Two-Factor Authentication Defends Against Fraud
http://www.gradian.co.uk/Resource_Lib/RSA/Protecting%20Against%20Phishing.pdf
13. "Paypal scam site using SSL spotted" Internet Storm Center Handler's Diary, 7 July 2003.
<http://isc.sans.org/diary.php?date=2003-07-07>

For additional information, also see the following:

The ePublic Eye site

<http://www.thepubliceye.com/eye2-1.htm>

Explanation of Bad Check Deposit Responsibility

http://www.fraudaid.com/ScamSpeak/Nigerian/counterfeit_check_fraud/counterfeit_check_03.htm

Copyright © 2005 infectionvectors.com. All rights reserved.

