

WHITEPAPER

Surefire Tips to Protect Yourself from Phishing

Knowledge is a powerful weapon in the fight against email fraudsters...
what you can do to avoid being caught by phishing scams
... The top 10 tricks used in phishing emails and fraudulent Web sites

Table of Contents

1. A Growing Threat to Consumers and Businesses	1
2. Surefire Tips to Protect Yourself from Phishing Scams	3
3. Top 10 Tricks Used in Phishing	4
4. Conclusion	16
5. About MailFrontier	17

1. A Growing Threat to Consumers and Businesses

“Phishing” is the most common type of fraudulent email today. *Phishing emails – so named because fraudsters use them to “fish” for information – attempt to entice people to provide sensitive information or take actions that a fraudster can exploit for financial gain or other malicious purposes.*

Until recently, phishing was a problem mainly for consumers. In a June 2004 report from research firm, the Gartner Group, the results of a consumer survey conducted in April revealed that 57 million Americans think they have received a phishing email. About 1.8 million of those who reported having received a phishing email said they responded, disclosing personal or financial information. Of those, half were the victims of some form of identity theft related fraud.

And the problem is growing. According to the Gartner survey, 76 percent of the phishing emails arrived within the prior six months and nearly all within the prior year. And almost all of the fraud resulting from phishing emails has happened in the past year, costing banks and card companies about \$1.2 billion in direct losses.

Flushed with success defrauding consumers, fraudsters now are turning their sights on businesses, having discovered that techniques that work well with consumers work equally well with unsuspecting employees. Phishing emails aimed at employees often appear to come from trusted sources such as company management or partners; use legitimate company graphics, layout, content and links; and ask employees to take actions that seem reasonable in a business context, such as verifying company information.

In fighting phishing emails, many organizations treat them as just another type of spam and in some ways, they do look and act like spam. Phishing emails come in unsolicited and tend to request something of the recipient such as a purchase, an action or an entry of information.

- But the similarity ends there and the differences are critical. While spammers and the emails they send are often blatantly authentic, fraudsters cloak themselves and their phishing emails as coming from a partner or friend. And while spammers often seek attention, fraudsters avoid it, masquerading as a trusted source and using your corporate email system and your employees against you

MailFrontier research further shows that in organizations using a spam filter to trap phishing emails, if the spam filter has no way of flagging email from an apparently trusted source that is, in fact, fraudulent, 40 percent of employees will remove it from quarantine, believing it to be legitimate. *This means that if 500 emails hit your corporate network requesting that your employees re-authenticate their network access information, and if your spam filter catches those emails, 200 recipients are likely to remove the email from quarantine and may act on it.*

Equally disconcerting, MailFrontier research shows that *1 out of 10 people who are shown a phishing email after they have been told it is suspicious are still fooled into acting upon it.*

You are at risk; but you can do something about it. Effective anti-phishing strategies start with knowledge – a powerful weapon in the fight against fraudsters. The more your employees know about how they are being targeted and what they should do when they suspect they have received a phishing email, the more likely they are to take appropriate action.

The more you know, the better prepared you can be.

In this whitepaper, MailFrontier – a market leader in email security that protects growing organizations from spam, virus, phishing, fraud and other email threats – presents surefire ways to protect yourself from phishing scams and the top 10 tricks used in phishing emails and fraudulent Web sites.

All of the examples used in this white paper are based on actual phishing emails and fraudulent Web sites, that have been forwarded to MailFrontier by our customers.

2. Surefire Tips to Protect Yourself from Phishing Scams

Email fraudsters go to great lengths to make their phishing emails appear to be from reputable companies and to hide their actual intent. And based on MailFrontier research, many fraudsters enjoy great success. In a MailFrontier online survey of more than 225,000 people who were shown 10 emails and asked to determine whether they were legitimate or fraudulent, participants responded incorrectly over 30 percent of the time¹.

Nevertheless, there are ways you can protect yourself from phishing scams.

Tip #1:

If you are not a customer of a company that appears to be sending you an email, ignore it.

Fraudsters rely on the few recipients who are customers of the company to fall victim to the scam.

Tip #2:

Even if you are a customer, never respond directly to an email request from a company for personal or financial information.

Instead verify the authenticity of the request by using an email or telephone contact that you know is legitimate.

Tip #3:

Never go to a web site from a link in an email.

Instead enter URLs that you know are legitimate directly into your browser or by using bookmarks you created.

Tip #4:

If an apparently legitimate Web site that you have visited before prompts you for a password, enter an incorrect one first.

A fraudulent Web site will accept an incorrect password while a legitimate one will not.

Tip #5:

If you unwittingly supply personal or financial information, inform the appropriate institutions immediately.

Banks and credit card companies will work with you to prevent your information from being used against you.

Tip #6:

Become familiar with the tricks of the trade so you can spot fraudulent emails.

Knowledge is a powerful weapon in the fight against email fraudsters.

¹To test your own phishing IQ, visit the MailFrontier Web site at www.mailfrontier.com.

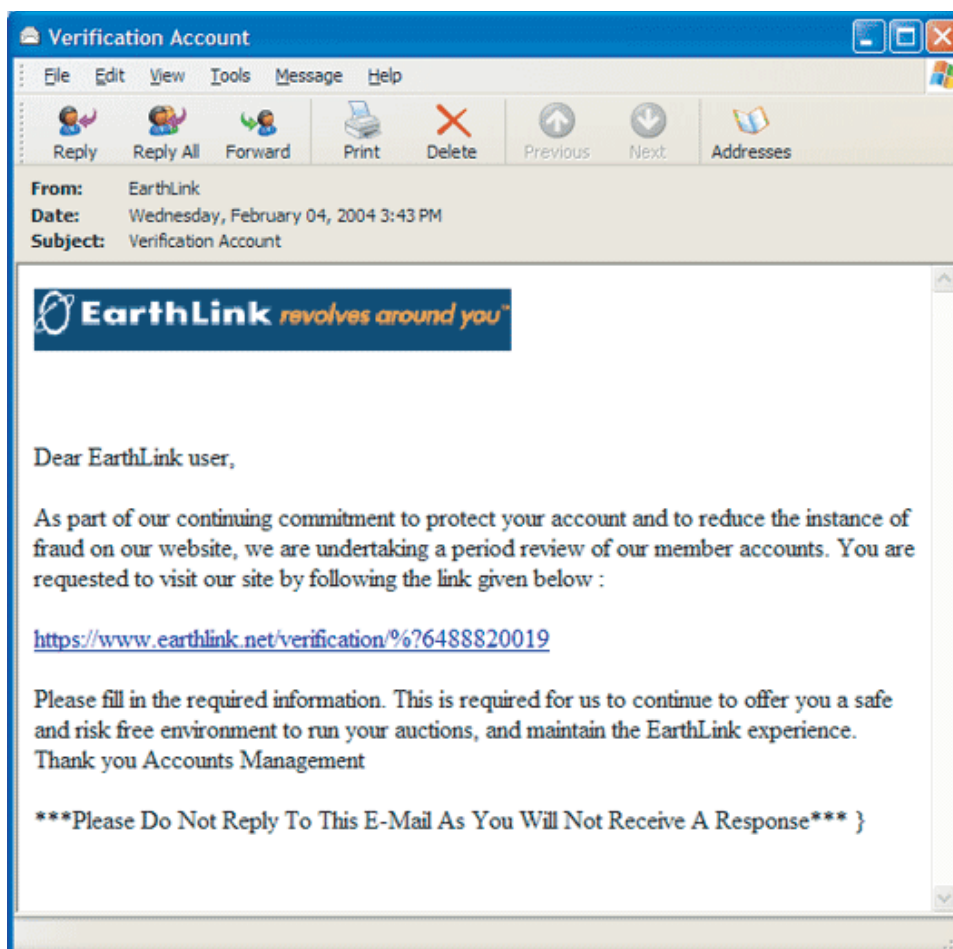
3. Top 10 Tricks Used in Phishing Emails

Why are phishing emails so difficult to recognize? Because fraudsters know they must gain your trust before you will respond or disclose personal or financial information. Here are some common tricks of the trade fraudsters use to make emails and Web sites look and act legitimate.

Trick #1: Mimic Reputable Companies

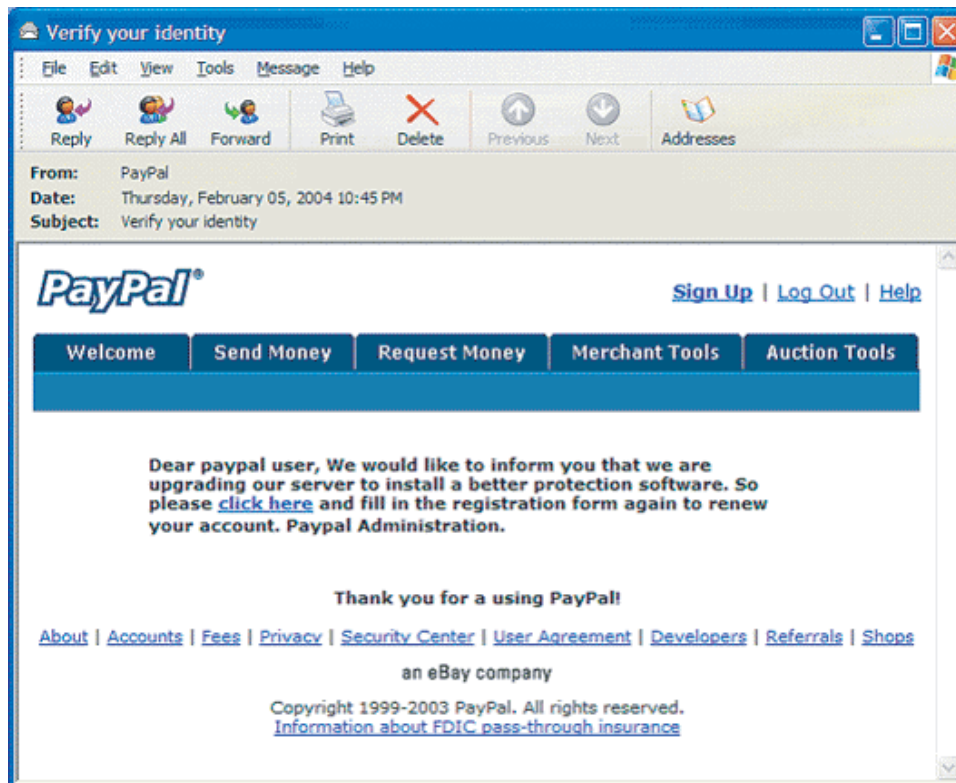
A successful phishing email will mimic or “spoof” a reputable company. The most targeted industry for spoofing is financial services and the companies spoofed most often are Citibank, eBay and PayPal. Internet retailers and Internet service providers also are frequent targets.

The most common way to mimic a reputable company is to adopt the company’s visible branding and corporate identity. In the email shown below, the fraudsters pulled the EarthLink logo from the EarthLink site.



While the main link in a phishing email sends the recipient to a fraudulent Web site, another way to add authenticity is to include links to sections of the real company's Web site.

In the fraudulent PayPal email below, all of the links in the email are linked to real PayPal Web pages except the "click here" link in the middle of the email text.

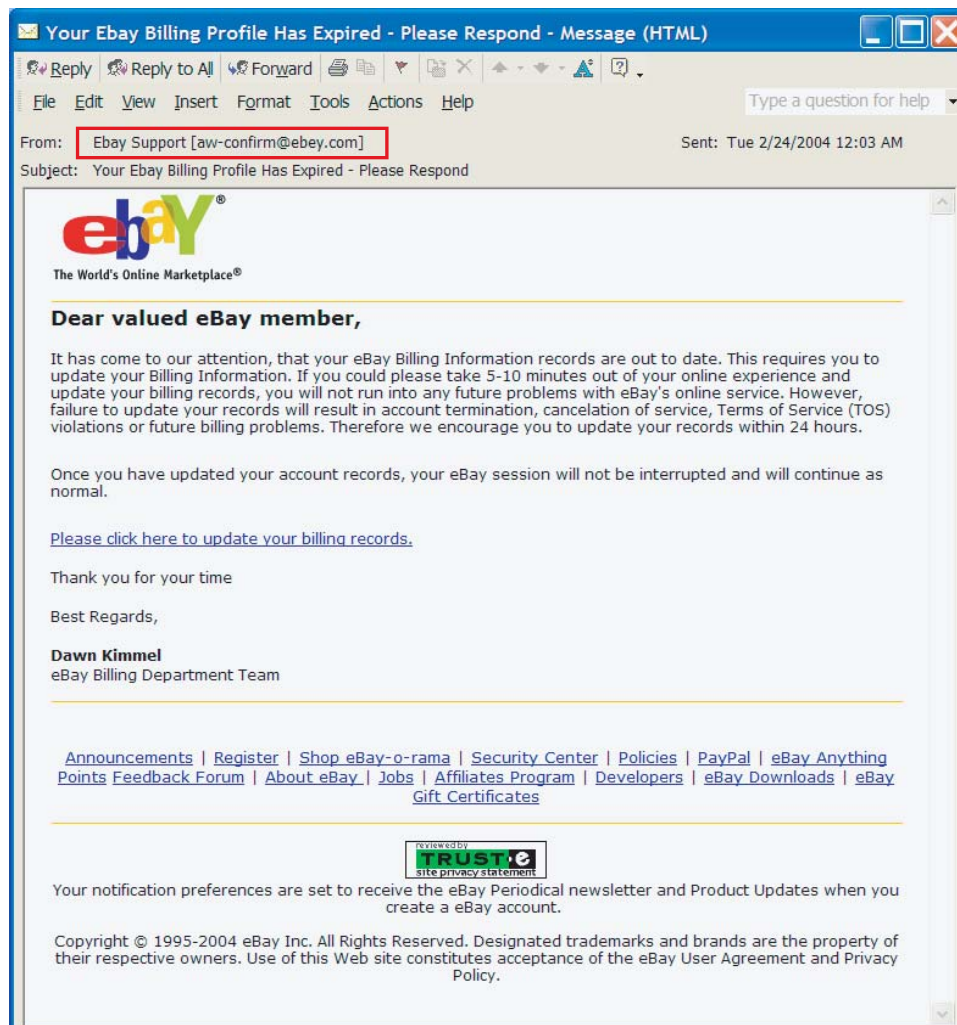


To further convince the recipient that the email originated from the reputable company, fraudsters use a "from" email address that appears to be from the company by using the company's domain name (e.g., @ebay.com, @paypal.com).

Trick #2: Use Different Reply Address From the Claimed Sender

In some phishing emails, the email claims to be from a reputable company, but is set to reply to a fraudulent reply address.

In the example below, this fraudulent eBay email claims to be from eBay support, but is set to reply to aw-confirm@ebey.com. Note that the fraudsters used "ebey" instead of "ebay."



Trick #3: Create a Plausible Premise

After convincing the recipient that the email originated from a reputable company, the email must present a plausible premise that persuades the recipient to divulge sensitive information. The email may claim that the recipient's account information is outdated, a credit card has expired or the account has been randomly selected for verification.

Ironically, the email often plays on people's fear of fraud to defraud them: The email may claim that the company has installed new security software and the recipient must renew the account information, or the email might claim that the account has been compromised by some sort of fraudulent activity and the account must be confirmed.

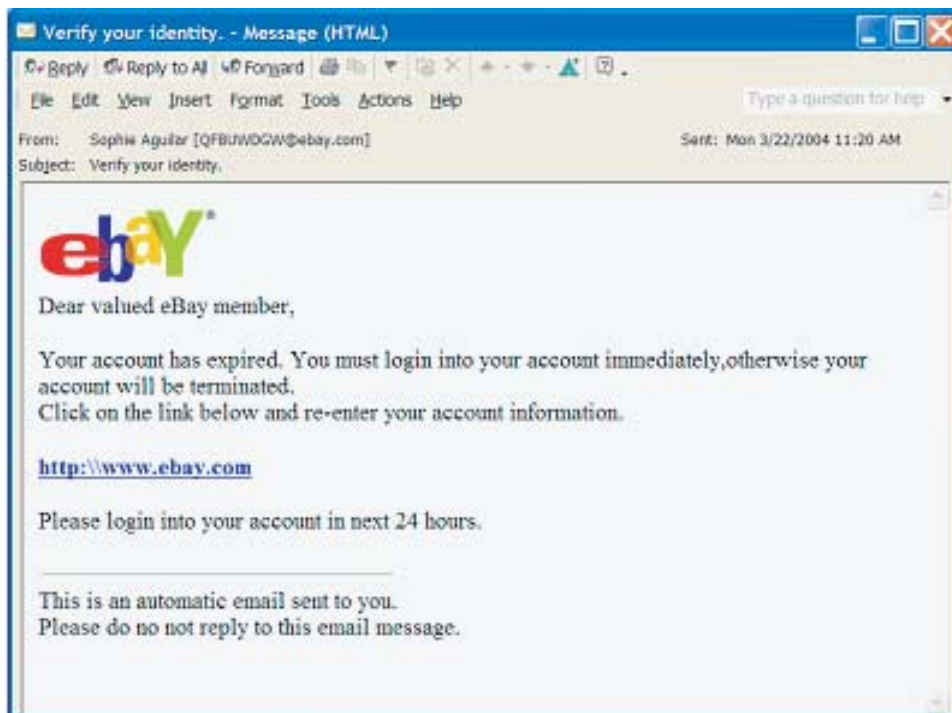
Trick #4: Require a Quick Response

Fraudsters have very little time to collect information before their sites are shut down, so they must convince the recipients to respond quickly. The following are examples of urgent requests sent in phishing emails:

"If you don't respond within 24h after receiving this Mail Information your account will be deactivated and removed from our server (your account suspension will be made due to several discrepancies in your registration information as explained in Section 9 of the eBay User Agreement.)"

"Please, give us the following information so that we could fully verify your identity. Otherwise your access to Earthlink services will be closed."

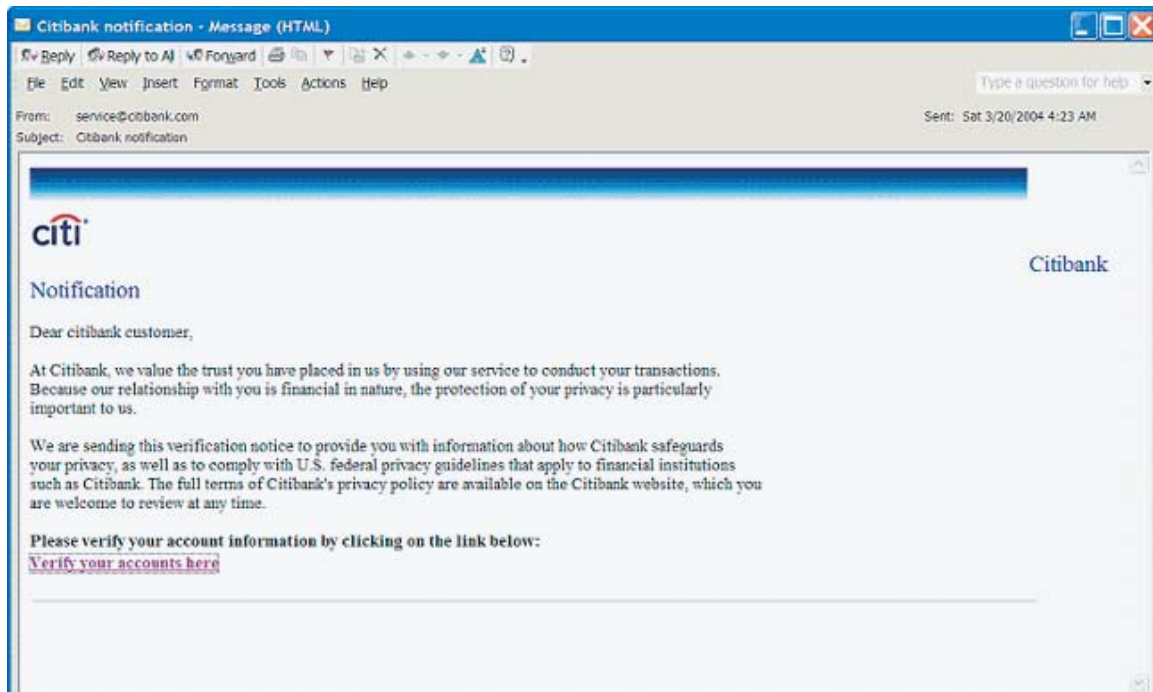
The fraudulent eBay email below claims that the recipient's account has expired and threatens to terminate the account if the recipient does not login through the link provided in the email within the next 24 hours.



Trick #5: Promise Security and/or Privacy

Phishing emails also try to assure the recipient that the transaction is secure and that their information will be kept private in hopes of gaining the recipient's trust.

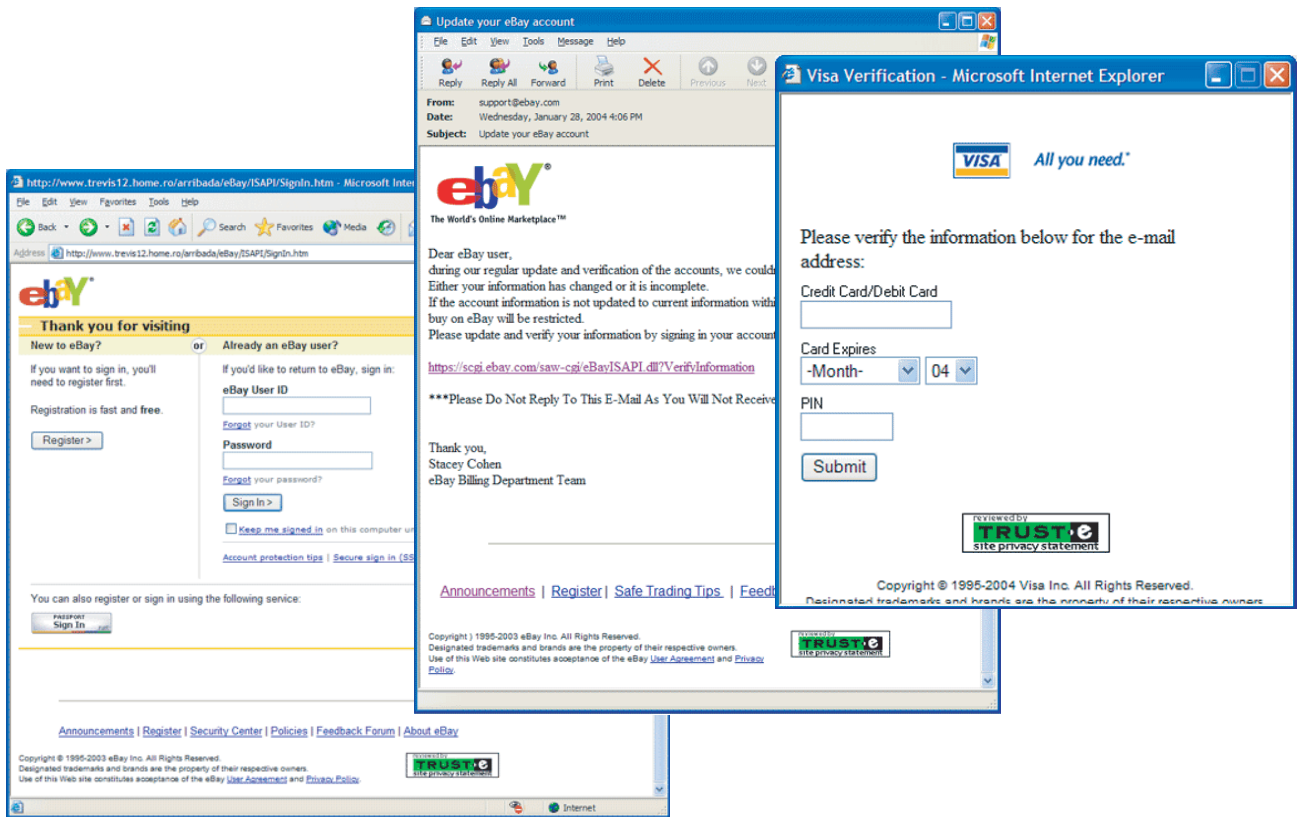
In the following fraudulent Citibank email, the fraudsters include the security assurance: "We are sending this verification notice to provide you with information about how Citibank safeguards your privacy, as well as to comply with U.S. federal privacy guidelines that apply to financial institutions such as Citibank. The full terms of Citibank's privacy policy are available on the Citibank website, which you are welcome to review at any time."



Phishing email messages also frequently use the TRUSTe symbol at the bottom of the email. The TRUSTe symbol is designed for use by businesses that agree to a high standard of personal information protection. (See <http://www.truste.org/>)



Here are some examples:



Trick #6: Collect Information in the Email


The earliest phishing emails used forms within the email to gather information. This method of phishing is still used in some of today's scams. Once the information has been entered, the email must provide a method of sending the information to the fraudster. Generally the "Submit" button at the bottom of the form sends the to the fraudster.

The image shows a screenshot of a web browser displaying an HTML email. The browser's address bar shows the title "Final notice - update your account to avoid service cancellation! - Message (HTML)". The email header includes "From: eBay.com [aw-confirm@ebay.com]" and "Subject: Final notice - update your account to avoid service cancellation!". The email content features the eBay logo and a warning: "Account Update with eBay Auction Community !!!". It states that the user's account information must be updated within 48 hours. A "Dear Valued eBay member," salutation is followed by a paragraph explaining the migration to better servers. A red "ATTENTION!" section warns that the account will be deleted if information is not sent by March 25th, 2004. Below this is a form with several sections: "eBay User ID" and "Password" (both with input fields); "Enter Credit Card/Debit Card Information" (with fields for Card Type, Credit card/debit card number, Expiration date, CVV2 Code, Debit card PIN/PIC, Birthdate, and Name of Cardholder); "Please enter billing address as it appears on your credit card bill statement:" (with fields for Billing address, Primary Phone, City, State/province, Zip/postal code, and Country); "Enter Bank Account Information" (with fields for Account owner, Country of account, Bank name, Bank routing #, Checking account #, Bank website, Bank username, and Bank password). A "Submit >" button is at the bottom of the form. Below the form is a checkbox for "Keep me signed in on this computer unless I sign out." and a footer with various links and a copyright notice for eBay Inc. 1995-2004.

Final notice - update your account to avoid service cancellation! - Message (HTML)

From: eBay.com [aw-confirm@ebay.com] Sent: Fri 3/3/2004 7:41 AM
Subject: Final notice - update your account to avoid service cancellation!

Account Update with eBay Auction Community !!!


The World's Online Marketplace® **Update Your Account Information Within 48 Hours**

Dear Valued eBay member,

We are moving to better servers so that better services can be provided. Due to our migration, it is necessary to update our database and backup our customer's data. In order for us to accomplish that, you need to enter the below information.

ATTENTION!
If this information is not sent to eBay by March 25th 2004, your eBay account with us will be automatically deleted!

All fields below are required. Please double check before you Submit

eBay User ID

Password

Enter Credit Card/Debit Card Information

Card Type:

Credit card/debit card number Credit Card: Visa, MasterCard, American Express, Discover. Debit Card: Visa, MasterCard.

Expiration date Month: Year:

CVV2 Code 3 Digit code at the back of your card; next to signature (American Express need 4 digits)

Debit card PIN/PIC The ultimate measure of security used at ATMs

Birthdate:

Name of Cardholder

Please enter billing address as it appears on your credit card bill statement:

Billing address

Primary Phone ()

City

State/province

Zip/postal code

Country

Enter Bank Account Information

Account owner First name Last name

Country of account

Bank name

Bank routing #

Checking account #

Bank website (ex: www.citibank.com)

Bank username


Bank password

Keep me signed in on this computer unless I sign out.

[Announcements](#) | [Register](#) | [Shop eBay-o-rama](#) | [Policies](#) | [PayPal](#)
[Feedback Forum](#) | [About eBay](#) | [Jobs](#) | [Affiliates Program](#) | [eBay Downloads](#)

[My eBay](#) | [Site Map](#)
[Browse](#) | [Sell](#) | [Services](#) | [Search](#) | [Help](#) | [Community](#)

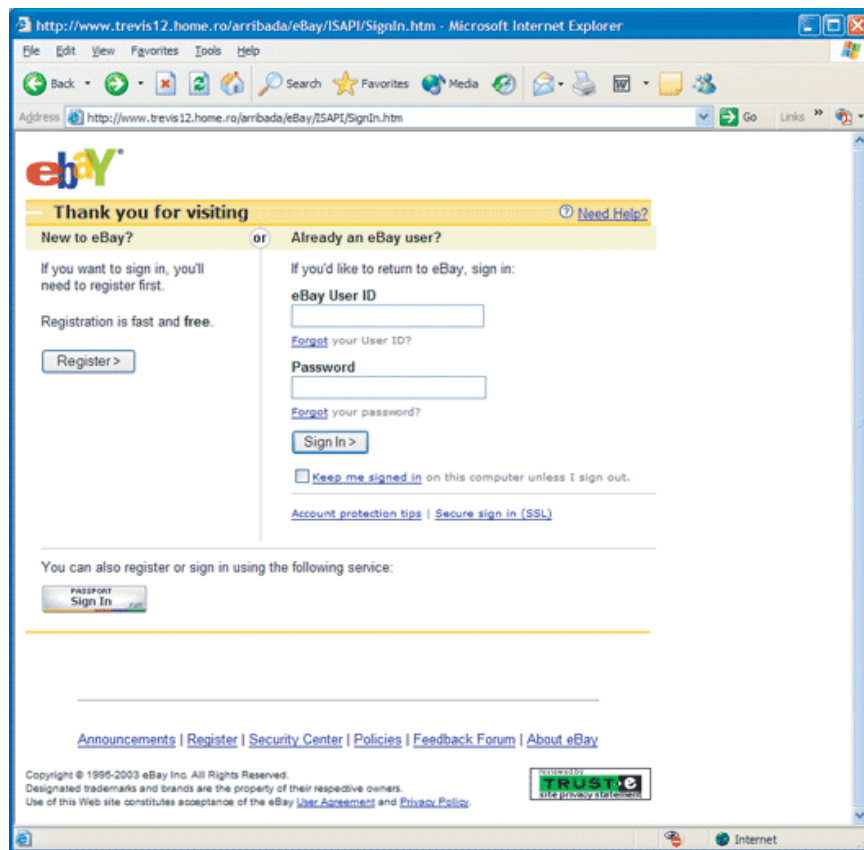
Copyright © 1995-2004 eBay Inc. All Rights Reserved.
Designated trademarks and brands are the property of their respective owners.
Use of this Web site constitutes acceptance of the eBay [User Agreement](#) and [Privacy Policy](#).



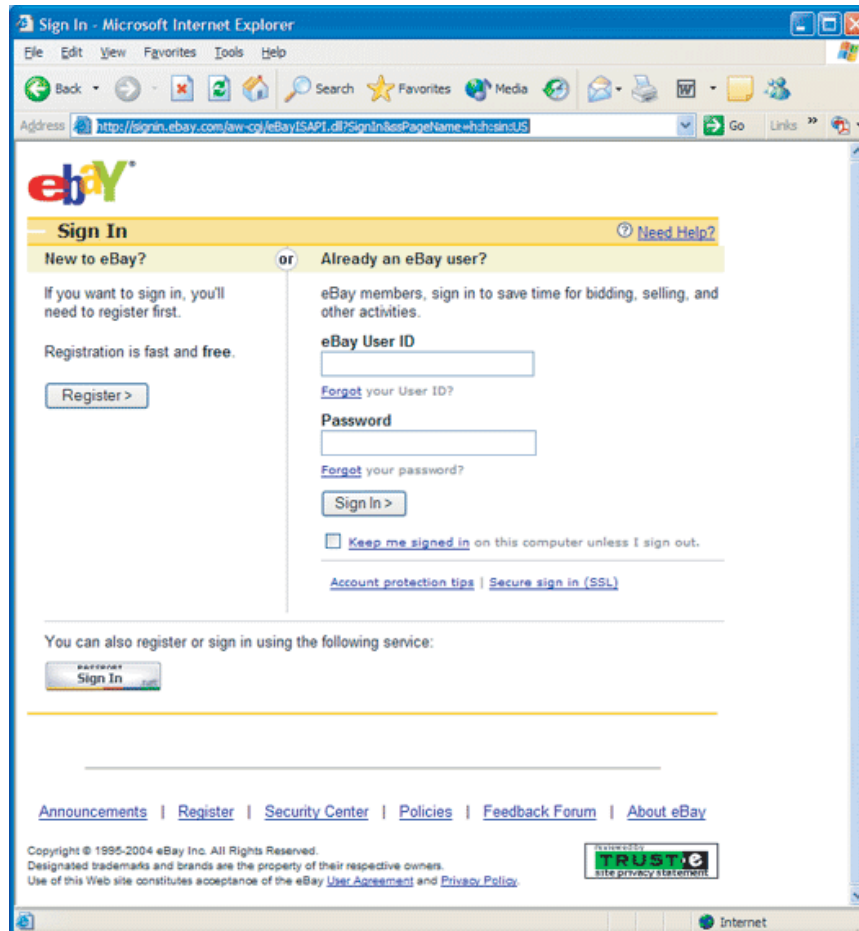
Trick #7: Link to Web Sites That Gather Information

Today, most phishing emails provide a link that takes the recipient to a fraudulent Web site instead of using forms within the email. Fraudsters continue to emulate the company they are spoofing in their fraudulent Web pages by using images from the company's real Web sites, similar fonts and color schemes. Some use the code from the real company's Web pages and merely change a few essential details, such as where the information is submitted or a link to forward the user to another fraudulent Web page. Some register domain names that are very similar to those owned by a reputable company in the hopes of fooling the recipient into believing that the URL is owned by a reputable company.

Many fraudulent Web pages look virtually identical to the real Web site, as in the example below.

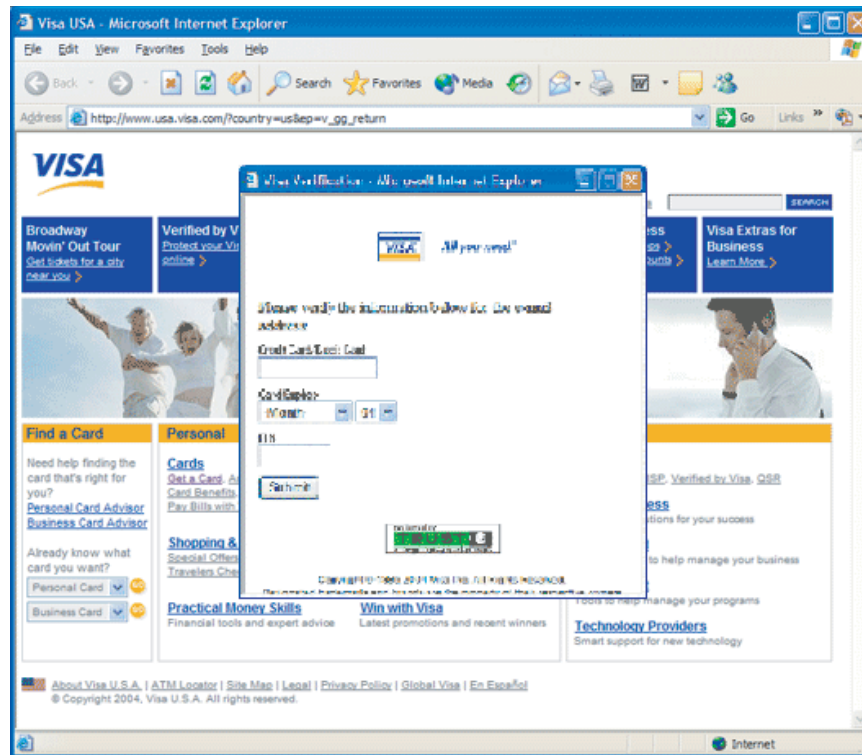


compare the fraudulent site on the previous page to the real eBay sign-in page below:



Once the recipient follows the link to the fraudulent Web site, the fraudster gathers information through forms. This process is similar to sending information through forms in emails, as discussed earlier. However, using Web pages instead of email forms provides fraudsters with more flexibility. Not only do the fraudulent Web pages have forms to gather information, many often contain introduction pages, pages indicating the information is being processed and pages thanking the recipient for the information. Frequently, the browser is redirected to the real company's Web site after the information has been collected in an attempt to further fool the recipient into believing that the request for the information came from the spoofed company.

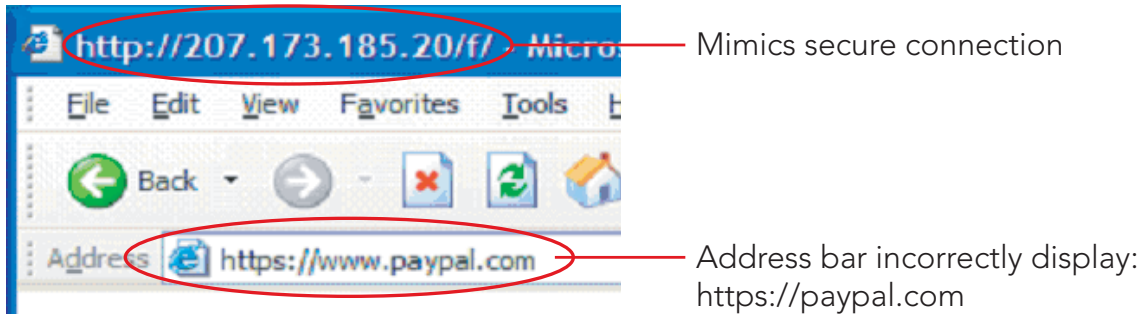
Many fraudulent Web pages are opened as pop-ups. Fraudsters cause the email link to go to the fraudulent Web site, which generates the fraudulent pop-up and then redirects the main browser window to the real company site. This transaction appears to the user as a pop-up over the real company site. Fraudsters use this technique to make their information gathering appear more credible.



Using a pop-up with the browser menu disabled discourages the viewer from saving the page. The viewer is limited to saving the source code by right clicking on the pop-up, selecting View Source and saving the code.

Trick #8: Fake a Secure Connection

A URL that begins with "https://" (instead of "http://") indicates that information is being transmitted over a secure connection and the company has been issued a Secure Sockets Layer (SSL) certificate. Some fraudulent sites use an "https://" URL to appear as a legitimate site. The following fraudulent PayPal site used this technique.



When recipients clicked on the appropriate link, they were directed to this security alert.



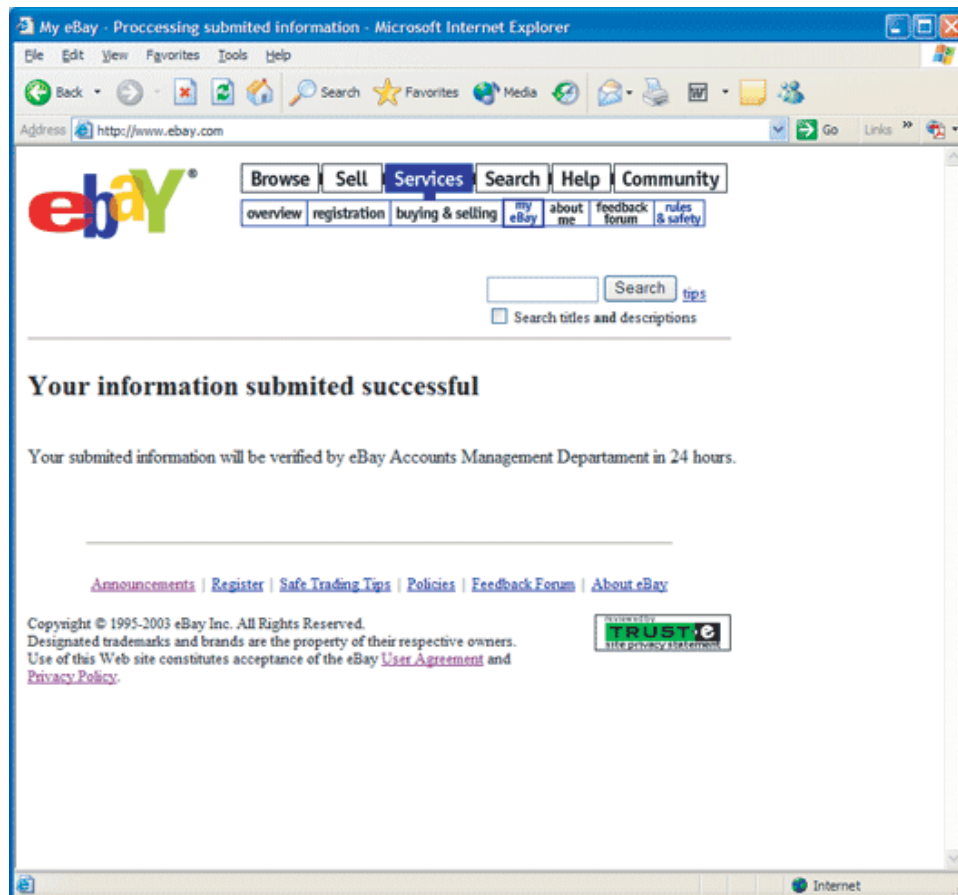
Most users are unsure what these alerts may indicate and these warnings are not uncommon when trying to access legitimate sites. Even with this warning, an invalid or fake certificate may make the user feel more secure in the transaction

Trick #9: Process Submitted Information Immediately

Some fraudulent Web sites process the information provided by the victim when the information is submitted. For example, some sites run credit card numbers to ensure they are valid, while others send the user ID and password information through the real company's site to verify that they are legitimate. If the user submits false or incorrect information, the page generates an error message. The Web site will not continue to the next step unless the user enters valid information.

Trick #10: Buy Time to Access Accounts

In some phishing scams, the fraudsters try to buy some time before their victims check on their accounts to give the fraudsters an opportunity to use the personal information they have acquired. The fraudsters indicate in either the email message or the Web pages that it will take a certain amount of time for the account to be updated. They hope that this will prevent their victims from checking their accounts during this time period. Here is an example.



4. Conclusion

Fraudsters go to great lengths today to devise effective ways to prey on unsuspecting consumers and businesses for personal and financial gain. And just as consumers and businesses continually change their practices to keep pace with emerging technology, fraudsters too adapt to the new opportunities that technology offers them.

Nevertheless, by understanding phishing as a distinct and sophisticated type of email threat, and by seeking solutions designed specifically to stop fraudulent email, you can protect yourself. The first step is knowledge, a powerful weapon in the fight against email fraudsters. Only by understanding the tricks of the trade used by fraudsters can we foil them.

To read more about how to protect your organization from phishing and other types of email fraud, visit www.mailfrontier.com and download the whitepaper: "Stop Email Fraud... Before it Stops You."

5. About MailFrontier

MailFrontier is an email security company that protects your organization from spam, virus, phishing, fraud and the growing number of other costly email threats. Fighting an enemy that changes daily, MailFrontier is a market leader, offering best-in-class protection from all known threats, blended attacks and new threats as they emerge. Only MailFrontier is effective and easy, and ensures that you stay a step ahead of email threats that can cripple your productivity, increase your liability and cause your IT costs to skyrocket.

MailFrontier is dedicated to serving growing organizations by delivering product, service and partner experiences that meet your unique requirements. The industries we serve include media & entertainment, insurance, financial services, utilities, healthcare, manufacturing, high technology and other sectors. We have more than 800 customers, including Pier 1 Imports, the San Francisco Giants, Wyndham Hotels & Resorts and Peet's Coffee & Tea.

For more information about MailFrontier, contact us at:

MailFrontier, Inc.
1841 Page Mill Rd.
Palo Alto, CA 94304
Phone: 650.461.7500
Fax: 650.461.7501
www.mailfrontier.com



1841 Page Mill Road
Palo Alto, CA 94304
886-3NO-SPAM
www.mailfrontier.com