Online Fraud Report

By National Cyber Security Alliance and Bank of America

May 2006

Executive Summary

While 80% of Americans who use the Internet, conduct financial transactions online, there's still widespread concern with becoming a victim of online fraud or identity theft. Consumers are especially concerned that fraudsters will lure them into entering sensitive information into a counterfeit web site, or a hacker will break into their computer and steal their financial information. As a result of these concerns, consumers have started to view all emails and web sites with great skepticism, and understand that just supplying a user identification and password may not be sufficiently safe. For more protection against fraud, consumers are more willing to adopt additional layers of login security.

Despite their fear of being duped by fake web sites and fraudsters, Consumers still feel very confident in their ability to recognize fake emails. In fact, 87% of survey respondents thought they could correctly identify a fake email. However, this perception did not quite match reality. When given various screenshot samples, 61% failed to identify a real or legitimate email. Instead, the majority of respondents simply categorized all the samples as fake.

In addition, consumers are susceptible to conducting transactions with unsecured or unsafe web sites, because they rely on a single symbol, such as a "padlock," to identify a secure web site. When asked, 67% of respondents failed to correctly identify a secured web site out of a number of samples. Instead, the majority of respondents wrongly identified an unsecured web site as secure, because the sample had a fake "padlock" certificate pasted in the middle of it.

Even though most respondents felt that legitimate web sites are responsible for protecting consumers from fake emails and web sites, respondents felt they themselves and Internet Service Providers played a shared role in combating online fraud. In addition, respondents did not feel very confident in using login IDs and passwords as the only way to protect themselves from Internet fraudsters. Online users are showing receptivity to additional security measures, such as personal questions beyond the traditional ID and password and technology that identifies a user's computer, as ways to secure and protect their financial information.

Executive Summary, *Continued*

Specific findings of the study include:

- Roughly eight in ten Americans that use the Internet, conduct online financial transactions, such as online banking, purchasing goods, stock transactions, or filing taxes.

- Two-thirds of consumers that conduct online financial transactions are extremely or very concerned about (1) giving their personal or financial information to a fake web site and (2) having hackers steal financial information from their computer.

- Even though 87% of respondents feel extremely or somewhat confident in their ability to recognize a fake email, 61% of them failed to correctly identify a real or legitimate email.

- 67% of respondents failed to correctly identify a secure and safe web site. Moreover, 58% of respondents are vulnerable to dealing with unsecured and unsafe web sites, because they rely on symbols like “padlocks” to tell them that a site is secure.

- 74% of Americans do not believe the current practice of using an ID and password to log-in is extremely or very safe; and, over 68% of respondents are extremely or very willing to try additional layers of login security, such as answering personal questions about themselves to confirm their identity.

- Over 4 out of 5 Americans believe that the responsibility of limiting and preventing online fraud is equally shared by legitimate web site, themselves and Internet Service Providers.

- Over 80% of consumers understand that not opening unsolicited emails, using the proper security software (anti-virus, anti-spyware and a firewall) and keeping security software updated are all ways to prevent Internet fraud. However, according to the 2005 AOL/NCSA Online Safety Study, 80% of consumers do not practice most of these key security measures.

Conducting Online Transactions

Q. Do you conduct online transactions via the Internet, such as online banking, purchasing goods, stock transactions or filing state or federal income taxes?

The vast majority of Americans who go online are conducting online financial transactions.

Eight in ten (82 %) of the respondents claim to conduct transactions, such as online banking, purchasing goods, stock transactions or filing state or federal income taxes, via their computers.

Concern With Financial Information In The Wrong Hands

Q. How concerned are you about the following (giving out financial information to a fake web site, having hacker steal financial information from your computer, having someone steal your bank account information while conducing business with reputable web site, contracting a virus or malicious program) taking place during online transactions?

Overall, the public is more concerned with the loss of financial information online than about viruses or malicious programs.

- Over two-thirds of the respondents are extremely or very concerned about giving their financial information to a fake web site (68 %). Approximately two-thirds are concerned on a top-two box level with having a hacker steal financial information (66 %) and having someone steal financial information while conducting business with a reputable web site (65 %). Concerns about viruses and malicious programs is last on the list (62 %).

- Women are significantly more concerned with all of the listed scenarios compared to men.

Online Fraud Responsibility

Q. Specifically regarding online transactions, whose responsibility is it to limit or prevent online fraud from fake emails or web sites asking for personal information while transacting online?

Overall, respondents say responsibility to limit or prevent online fraud falls on the legitimate web site and themselves. Women more so than men feel the Internet Service Provider is responsible.

- Nearly nine in ten respondents feel limiting or preventing online fraud is up to the legitimate/real web site (87 %). Over eight in ten say the responsibility also falls on themselves (83 %).

- Women are significantly more likely to agree strongly or agree somewhat that the Internet Service Provider should be responsible for limiting or preventing online fraud from emails or web sites (82 % versus 76 %).

- The government is thought to have far less responsibility.

Reasons for Level of Personal Responsibility

Q. Why do you feel this way?

The majority of respondents put some burden on themselves when it comes to preventing online fraud.

- When it comes to taking personal responsibility, respondents mentioned reasons, such as: 1) It's my responsibility to know who I'm dealing with, 2) You shouldn't supply information over the Internet, 3) I'm responsible for my information, 4) Don't answer mail unless familiar with the sender, and 5) Make sure the site is legitimate.

Confidence In Ability To Identify Fake E-Mail

Q. How confident are you in your ability to recognize a fake email asking for personal information?

Roughly half of internet users feel extremely or very confident in their ability to discern a fake email.

- 48 % of respondents feel extremely or very confident in their ability to recognize a fake email for personal information.
- Somewhat more men than women rated their confidence high (51 % versus 45 %).

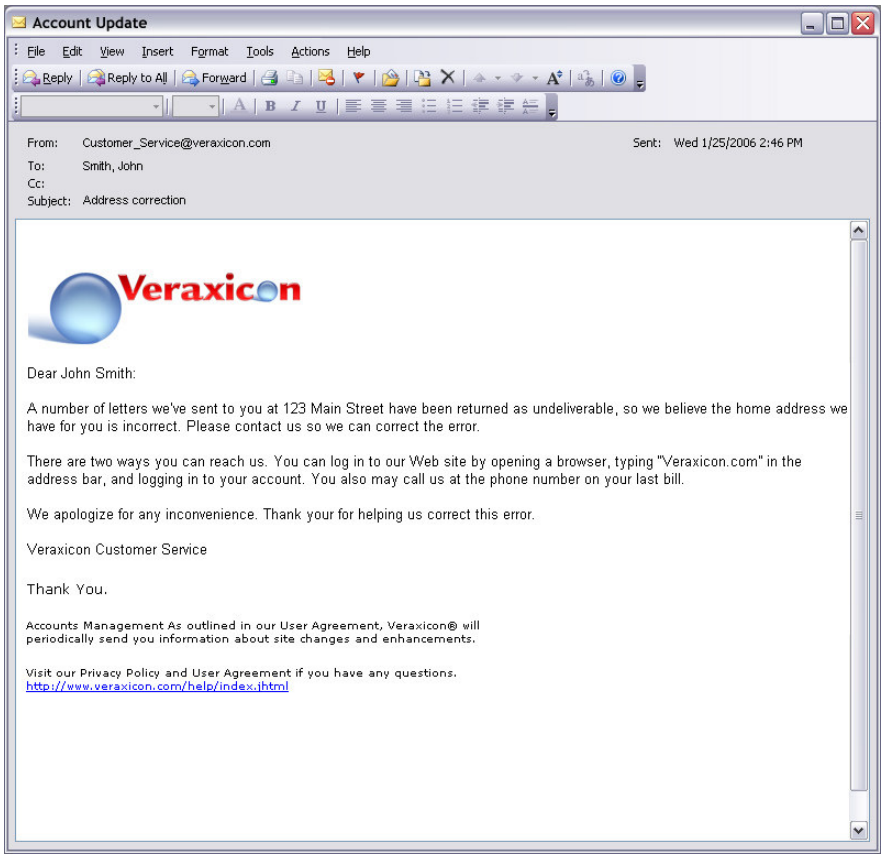
Email Authenticity Rating

Q. Based on your experience and what you know, please indicate how real or authentic each of these emails are. (See example e-mails on the next page.)

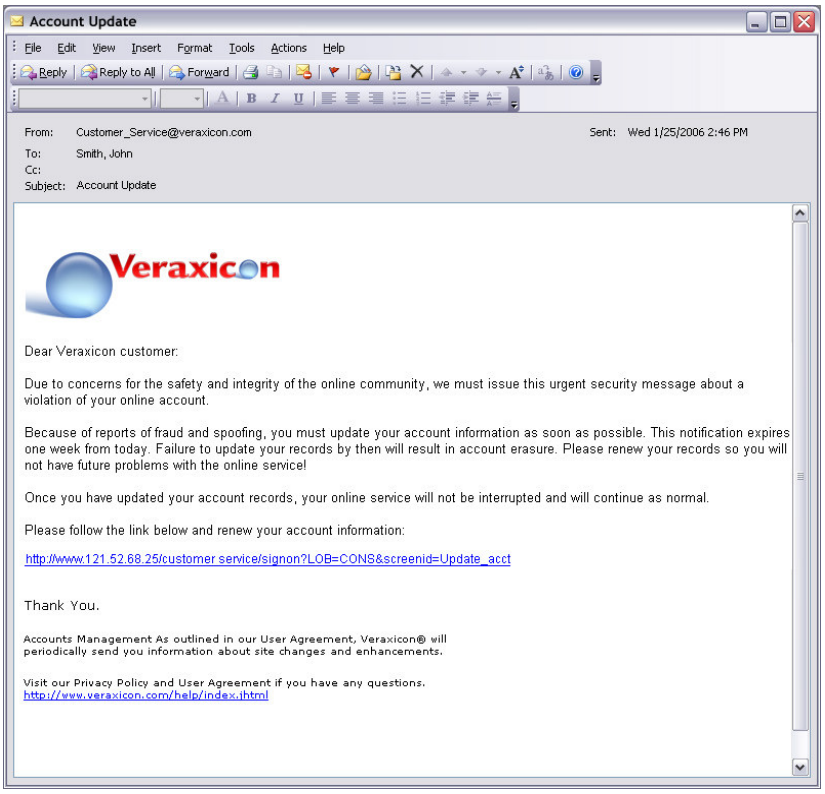
When presented with unfamiliar e-mails – including legitimate e-mails – online Americans are highly skeptical, although more rated the real email as legitimate.

- Only four in ten respondents saw the real email as extremely or very authentic in their eyes (39 %). Less than one in ten respondents rated the fake emails as authentic.
- Men and women rated the examples similarly.

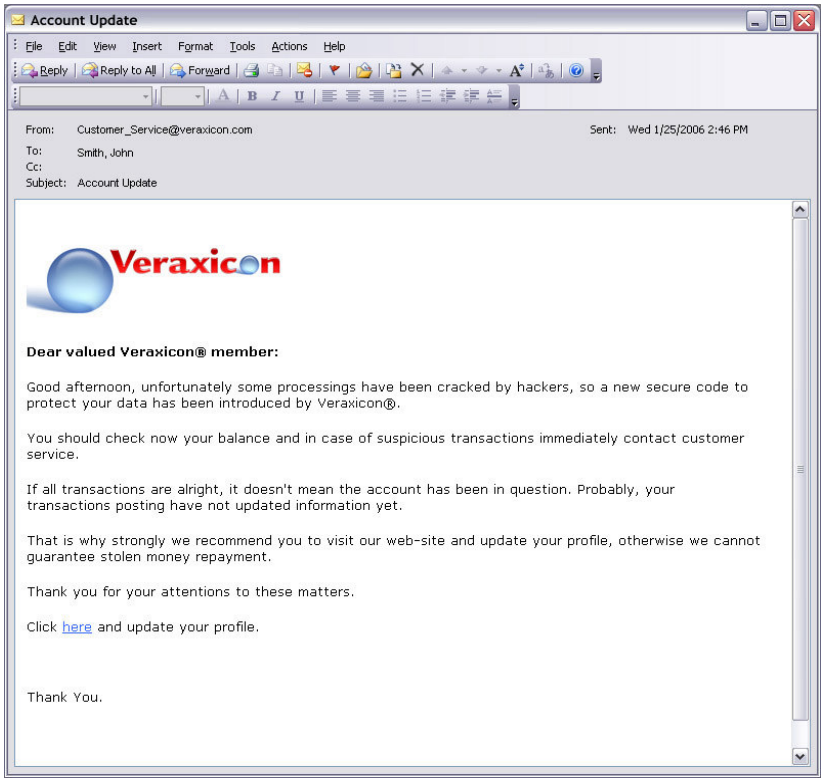
Email Example 1:



Email Example 2:



Email Example 3:



Web Page Safety Rating

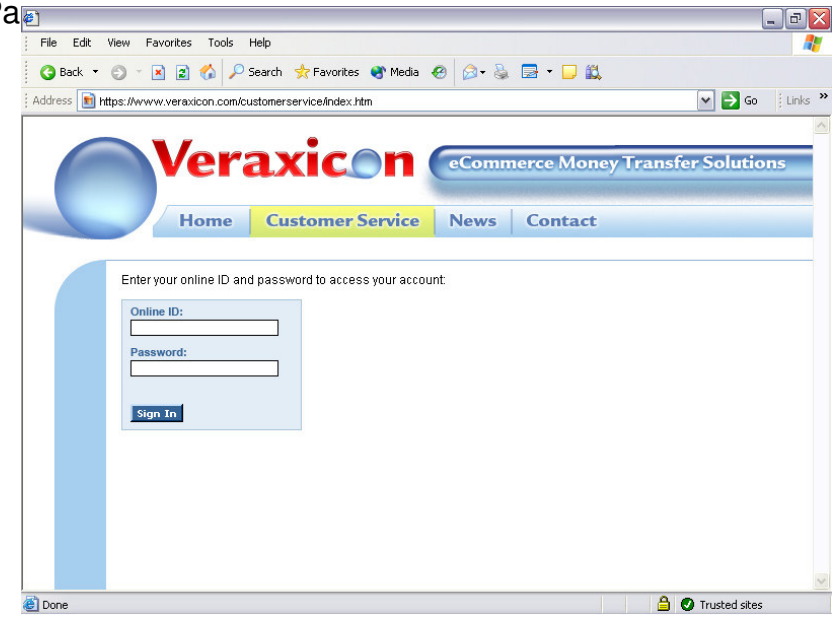
Q. Based on your experience and what you know, please indicate how safe it would be to provide personal information on each of these web pages. (See example web pages below.)

When presented with unfamiliar web pages - respondents were generally highly skeptical of their safety.

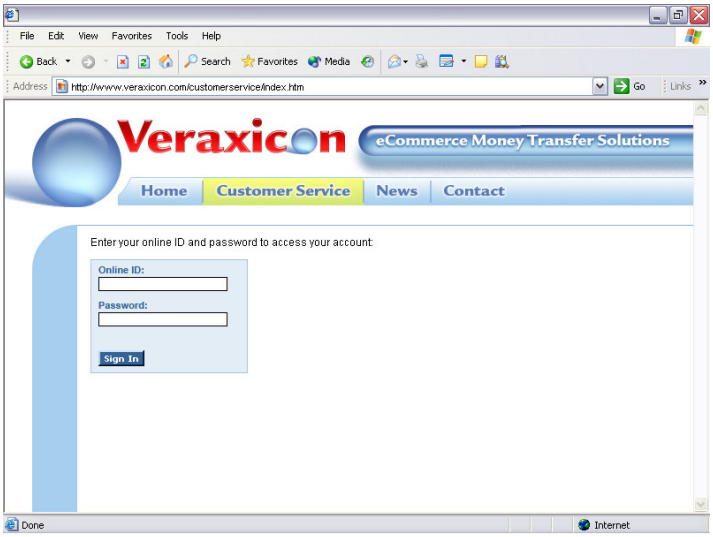
- Only one-third of the respondents saw the real web page as extremely or very safe (33 %) whereas nearly three in ten respondents rated one of the fake web pages as extremely or very safe (27 %).

- Women were significantly more likely to rate the fake web page (N-W2: no https or lock; IP address not URL; fake digital certificate) as secure.

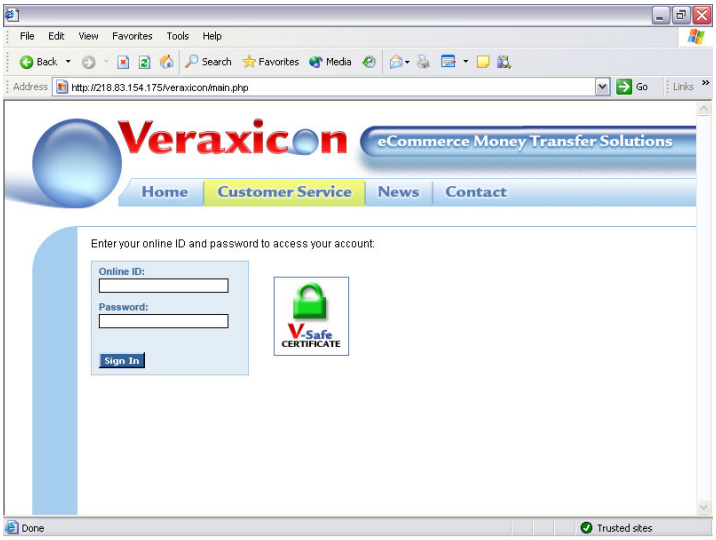
Web Pa



Web Page Example 2:



Web Page Example 3:



Web Page Example 4:

Web Page Safety Know-How

Q. How do you know that it is safe to provide personal information on a web site?

People are most likely to rely on a symbol (such as a padlock) to indicate a safe site. However, a large number say there is no real way to tell if a site is secure.

- Nearly six in ten respondents rely on symbols to tell them that a site is secure (58 %). Over four in ten respondents feel there is no real way to tell for sure (43 %). And over one-third of the public feel the clear contact information on the web site (36 %) and typing in the web address personally (33 %) makes them certain the site is safe.

- Women were more likely to claim the padlock symbol (62 % versus 54 %), clear contact information (41 % versus 32 %) and asking a friend (9 % versus 3 %) as ways to verify the safety of a web site. On the other hand, men are more likely to believe the “https” in the web address tells them that the web site is safe.

Online Fraud Prevention Know-How

Q. Which of the following are ways to help prevent online fraud from things like fake emails or fake web sites?

Not opening emails from unknown senders, security software, not sharing passwords and keeping software updated are the most common ways respondents believe online fraud can be prevented.

- Over eight in ten respondents say not opening emails from unknown senders (89 %), using security software (88 %), not sharing passwords (86 %) and keeping software updated (84 %) are a few ways they prevent online fraud. Still another seven in ten avoid web sites that do not look real (71 %).

- Women more so than men will not open an email unless they know who the sender is (93 % versus 85 %).

Contact In Case of Online Fraud

Q. If you think you are the victim of online fraud, like from a fake email or web site, who should you contact?

Online users would be most likely to contact the legitimate institution if they receive an e-mail they know is fake.

- Over six in ten respondents say if they fell victim to online fraud they would contact the real or legitimate institution that was being imitated (63 %). At least half say they would contact law enforcement (53 %) or a government agency (49 %.)

- Men say they would contact the legitimate institution more so than women (66 % versus 59 %).

Login Safety Rating

Q. Please indicate your level of agreement on how safe you think the current practice is of having a user ID and password as a security process for logging onto web sites. Would you say it is…

Relatively few Americans feel that the current practice of having a user id and password is extremely or very safe.

- One-quarter of the respondents feel the current practice of using an ID and password is extremely or very safe (26 %).

Willingness To Adopt Additional Security Measures

Q. Most web sites ask you to provide a user ID and a password. There are a variety of ways to add more security. Please indicate your willingness to participate in these types of additional security on the sites where you conduct online transactions (such as online banking, purchasing goods, stock transactions or filing state or federal income taxes).

Additional security in the form of a personal question that gives details about favorite color or high school mascot is clearly more acceptable than the other security measures offered.

- Over two-thirds of the respondents are willing to add a personal question about themselves to the security lineup (68 %). Over four in ten are willing to add technology that would recognize their computer (46 %) and a phone call to further verify their identity (41 %).

- Men are more in favor of a device that gives them a password to complete the login process (41 % versus 34 %).