Identity Theft

Markus Jakobsson
Palo Alto Research Center

Alex Tsow[†]
The MITRE Corporation

Identity theft is commonly defined as unwanted appropriation of access credentials that allows creation and access of accounts and that allows the aggressor to pose as the victim. Phishing is a type of identity theft that is perpetrated on the Internet and that typically relies on social engineering to obtain the access credentials of the victim. Similar deceit techniques are becoming increasingly common in the context of crimeware. Crimeware, in turn, is often defined as economically motivated malware. Whereas computer science has a long-term tradition of studying and understanding security threats, the human component of the problem is traditionally ignored. In this chapter, we describe the importance of understanding the human factor of security and detail the findings from a study on deceit.

Social engineering can be thought of as an establishment of trust between an attacker and a victim, where the attacker's goal is to make the victim perform some action he would not have wanted to perform had he understood the consequences. Attackers leverage preexisting trust between victims and the chosen false identities to spur dubious actions (illegally transferring money, remailing stolen goods, installing malware on computers, and recommending fraudulent services to friends).

To understand deceit in this context, it is worth recalling that people are more likely to install software on their computer if they believe it is manufacturer-distributed patch rather than a third-party enhancement. Similarly, Internet users are more likely to visit a website when recommended by friends[1,2] and may agree to signing up to services that appear to be recommended by their friends. Moreover, when site-content hinges on accepting third-party browser extensions, friend recommendations prove highly effective in inducing the required installation.[3] When identity is used convincingly, these behaviors become social vectors for spreading crimeware and for causing users to opt in where they would not otherwise have.

Institutions and individuals project Internet identity through their Web sites and through email communication. How do attackers engineer contact with false identities? Clearly, email can be sent to anyone. Filters limit the quantity of unwanted messages, but spammers have successfully responded with increased volume and variation. Superficially, arranging contact with bogus Web sites appears to be a more difficult problem since legitimate content providers uncommonly link to spoofed Web hosts.

Roughly 50% of Web requests (by volume) are not the result of site-to-site linking, based on results from over 100,000 Internet clients hosted by the Indiana University campuses, according to the Indiana University Advanced Network Management Lab.

The other half of Web visits follow from bookmarks, direct address bar manipulation, or linking from external sources (email, word-processor documents, and instant-

[†] The author's affiliation with The MITRE Corporation is provided for identification purposes only, and is not intended to convey or imply MITRE's concurrence with, or support for, the positions, opinions or viewpoints expressed by the author.

[1] T. Jagatic, N. Johnson, M. Jakobsson, and F. Menczer, "Social phishing," *Communications of the ACM*, 2007, available at http://doi.acm.org/10.1145/1290958.1290968.

[2] A. Genkina and L. J. Camp, "Phishing and countermeasures: understanding the increasing problem of electronic identity theft," chapter case study: *Net Trust*, John Wiley & Sons, 2007.

[3] M. Gandhi, S. Stamm, M. Jakobsson, "verybigad.com: A study in socially transmitted malware," www.indiana.edu/~phishing/verybigad/.

messaging sessions). Social engineers influence these values through bogus links in email and by using domain names that are deceptive.

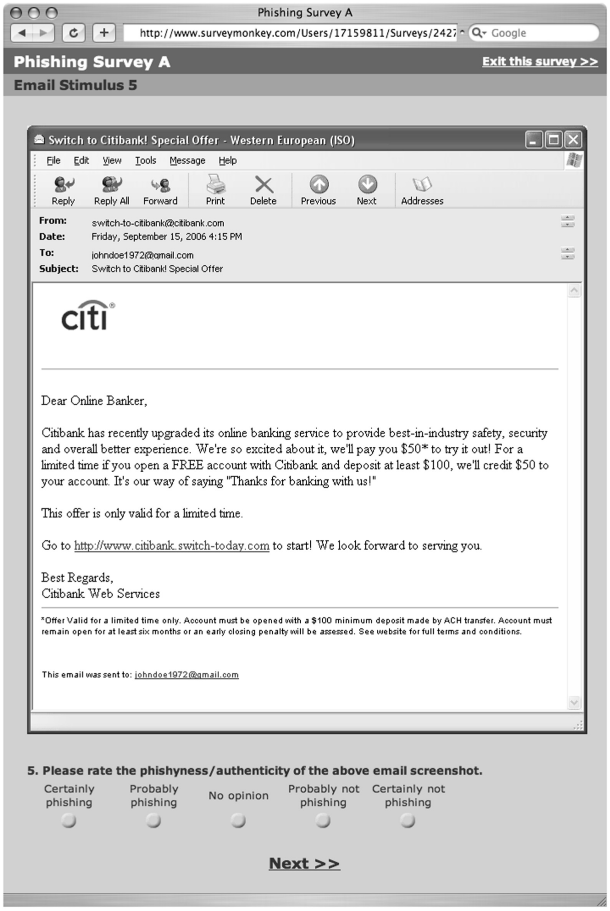
There are may studies of ways in which humans relate to deceit and treason, and there are many studies that focus on Internet security, but there is not an abundance of research on the combination of these two important fields. How do people relate to deceit on the Internet? This is an important question to ask—and to answer—for anybody who wants to improve Internet security.

1. EXPERIMENTAL DESIGN

This experiment tests the ability to identify phishing, an Internet scam that spoofs emails and Web pages to trick victims into revealing sensitive information. Although cast in terms of phishing, the results generalize to identity spoofing for purposes beyond information theft. This experiment tests the effects of several media features—sometimes in multiple contexts—on an individual's evaluation of its phishing likelihood. This experiment shows subjects six email screenshots followed by six Web page screenshots and asks them to rate their authenticity on a five-point scale: Certainly phishing, Probably phishing, No opinion, Probably not phishing, and Certainly not phishing (see Figure e49.1 for an example). The experiment was administered through SurveyMonkey.com,[4] an online Web survey service. Subjects were required to rate each screenshot before advancing to the next stimulus. The survey provided the following instructions to subjects:

- Phishing is a form of Internet fraud that spoofs emails and Web pages to trick people into disclosing sensitive information. When an email or Web page fraudulently represents itself, we classify it as phishing.
- This survey displays a sequence of email and Web site screenshots. Assume that your name is John Doe and that your email address is johndoe1972@gmail.com. Please rate each screenshot's authenticity using the five-point scale: Certainly phishing, Probably phishing, No opinion, Probably not phishing, Certainly not phishing.

This style of testing, termed *security first*, measures fraud-recognition skills rather than habits. Subjects are not trying to accomplish other work but are merely instructed to rate a series of legitimate and illegitimate stimuli. For this reason, security-first measurements place a plausible upper bound on fraud detection habits in normal computer usage. Even though security-first evaluations have shown high susceptibility to phishing,[5,6] role-playing experiments designed to measure fraud detection habits[7,8] demonstrate even more serious vulnerability.


Phishing Survey A
http://www.surveymonkey.com/Users/17159811/Surveys/2427
Google
Phishing Survey A
Exit this survey >>
Email Stimulus 5
Switch to Citibank! Special Offer - Western European (ISO)
File Edit View Tools Message Help
Reply
Reply All
Forward
Print
Delete
Previous
Next
Addresses
citi

From: switch-to-citibank@citibank.com
Date: Friday, September 15, 2006 4:15 PM
To: johndoe1972@gmail.com
Subject: Switch to Citibank! Special Offer

Dear Online Banker,

Citibank has recently upgraded its online banking service to provide best-in-industry safety, security and overall better experience. We're so excited about it, we'll pay you $50* to try it out! For a limited time if you open a FREE account with Citibank and deposit at least $100, we'll credit $50 to your account. It's our way of saying "Thanks for banking with us!"

This offer is only valid for a limited time.

Go to http://www.citibank.switch-today.com to start! We look forward to serving you.

Best Regards,
Citibank Web Services

*Offer Valid for a limited time only. Account must be opened with a $100 minimum deposit made by ACH transfer. Account must remain open for at least six months or an early closing penalty will be assessed. See website for full terms and conditions.

This email was sent to: johndoe1972@gmail.com

5. Please rate the phishyness/authenticity of the above email screenshot.

Certainly phishing	Probably phishing	No opinion	Probably not phishing	Certainly not phishing
○	○	○	○	○

Next >>

FIGURE e49.1 Subjects evaluate authenticity based on Screenshots using a five-point scale. The survey required a judgment before proceeding to the next stimulus.

Subjects were recruited from an undergraduate introductory noncomputer-science-major class on computer usage and literacy. Of a class size exceeding 600 students, 435 began this study. All but 12 subjects were between

[4] SurveyMonkey.com, "Surveymonkey.com-powerful tool for creating web surveys. online survey software made easy!" www.surveymonkey.com/, retrieved December 2006.

[5] A. Genkina and L. J. Camp, "Phishing and countermeasures: understanding the increasing problem of electronic identity theft," chapter case study: *Net Trust*, John Wiley & Sons, 2007.

[6] M. Jakobsson, A. Tsow, A. Shah, E. Blevis, and Y.-K. Lim, "What instills trust? A qualitative study of phishing," In submission, 2006.

[7] J. S. Downs, M. B. Holbrook, and L. F. Cranor, "Decision strategies and susceptibility to phishing," In *SOUPS '06: Proceedings of the Second Symposium on Usable Privacy and Security*, pp. 79−90, New York, 2006, ACM Press.

[8] M. Wu, R. C. Miller, and S. L. Garfinkel, "Do security toolbars actually prevent phishing attacks?" In *CHI '06: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pp 601−610, New York, 2006, ACM Press.

17 and 22 years old; the gender split was 40.0% male to 57.9% female (2.0% did not respond to this question). Although the test population is not demographically representative of general computer users, their enrollment in the introductory course suggests that their computer skill level is generally representative. The class's only prerequisite is high-school algebra. Almost all students in this class had used computers before but had no particular expertise.

The experiment divided the population into two sets through random selection. The two sets completed different versions of the survey. For 10 of the stimuli, the two versions differ only by a target collection of test features. Our primary analysis compares the impact of the feature changes, by using the χ[9] to represent the difference between response distributions. In two other question sets, subjects evaluate the authenticity of messages and Web pages under third-party administration (a potential vector for social engineering). We further designed the test to simulate a roughly equal number of authentic and phishing stimuli to avoid effective use of a trivial rating strategy: If there were significantly more phishing stimuli than authentic stimuli, subjects could employ an "always phishing" strategy that would correctly evaluate most of the stimuli without exercising due consideration.

Since the stimuli are only screenshots, their inauthentic features were designed to be evident on examination (rather than mouse-over or source analysis). For instance, incorrect domains are apparent in email hyperlinks; they are not disguised by an inconsistent *href* attribute. The domains we chose to simulate inauthentic URLs were not in use at the time of testing, but some are owned by their respective companies, others are owned by unrelated companies, and the rest appear to be unregistered, according to the Whois database. Our use of these domains as representations of inauthentic URLs is still valid because none of these URLs exist with the content we present. We outline the stimuli, their relevant features, and what we hope to learn in Figures e49.2a and e49.2b.

Authentic Payment Notification: Plain versus Fancy Layout

These two email messages use actual payment notification text from Chase Bank (see sidebar, "A Strong Phishing Message"). The text personalizes its greeting and references a recent payment transaction; there are no hyperlinks. One version uses the original layout (a one-color header containing the company logo followed by the message text); the other version uses an enhanced layout (a header that includes a continuous tone shiny logo and a photograph of a satisfied customer, a smooth gradient footer graphic that spans the page with a gentle concave arch, hyperlinks to Privacy and Terms of Use, and a copyright notice; these graphics were adapted from the Web page at www.bankone.com).

A Strong Phishing Message

Dear John Doe,

JPMorgan Chase & Co. is proud to serve you as a former Bank One client.

Chase Online's patented ePIN technology is used both for eDebit transactions and for physical ATM access. While we will support the legacy 4 digit PIN for the remainder of the year, until December 31, 2006, we invite you to register for the ePIN program through our secure online server:

https://www.chase.ePIN-simplicity.com

If you have any questions about this or other Chase programs, do not hesitate to call our toll-free customer service number, 1-877-CHASEPC.

Sincerely,
Client Services
JPMorgan Chase & Co.

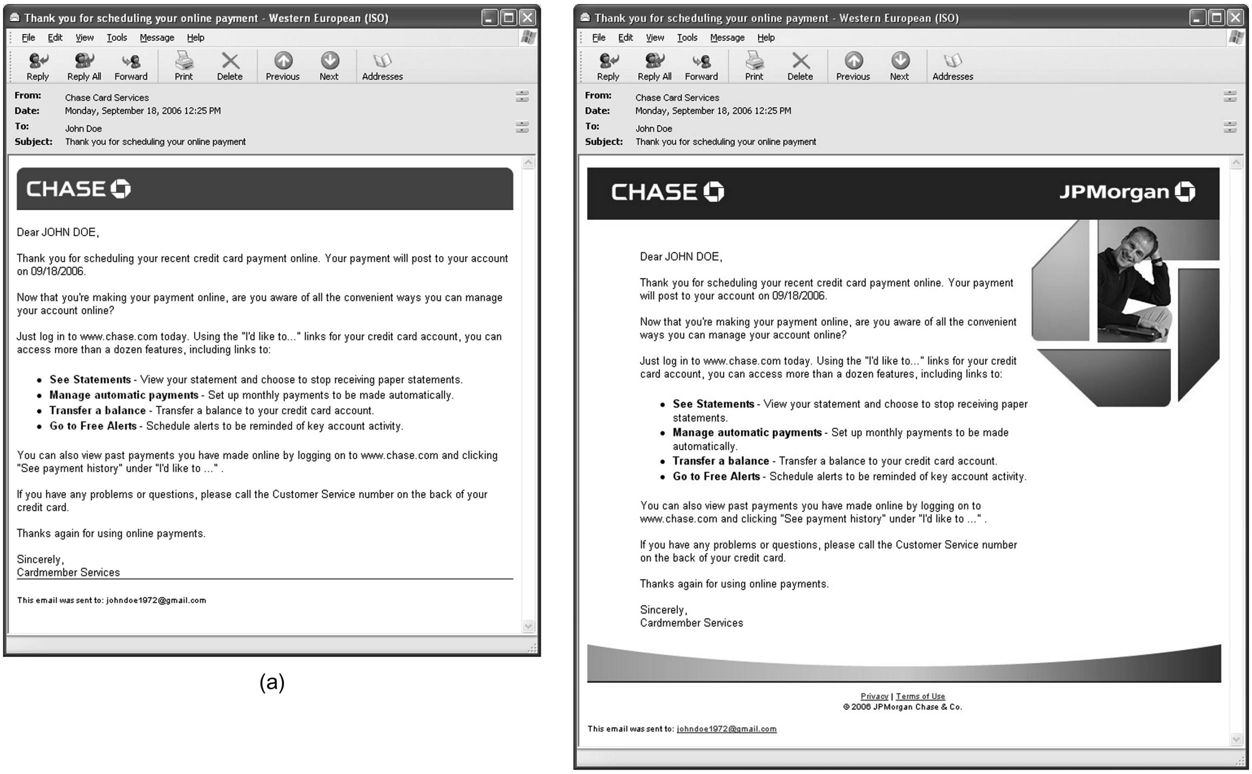
Strong Phishing Message: Plain Versus Fancy Layout

We constructed the phishing message text to sound as plausible as possible. Opening with a personalized greeting, the message explains that former Bank One customers will need to register for Chase's ePIN program—a replacement for ATM PINs that is also bundled with a new eDebit online service. It implicitly threatens service discontinuation by supporting "legacy 4 digit PINs for the rest of the calendar year." The bogus registration hyperlink uses the made-up URL https://www.chase.ePIN-simplicity.com. The message closes with a bogus phone number to call for assistance. The two versions of this message use the same plain and fancy layout schema described earlier, with one exception: The fancy layout adds shiny letters proclaiming "Bank One is now Chase" (see Figure e49.3) between the header and message text.

Authentic Promotion: Effect of Small Footers

Figure e49.4 shows an authentic message from the AT&T Universal card that promotes the company's paperless billing system. It personalizes the greeting and includes the last four digits of the account number. There are multiple company logos, a blue outline around text, an Email

[9] R. Dhamija, J. D. Tygar, and M. Hearst, "Why phishing works," In *CHI '06: Proceedings of the SIGCHI conference on Human Factors in computing systems*, pp. 581–590, New York, 2006, ACM Press.


Thank you for scheduling your online payment - Western European (ISO)
File Edit View Tools Message Help
Reply Reply All Forward Print Delete Previous Next Addresses

From: Chase Card Services
Date: Monday, September 18, 2006 12:25 PM
To: John Doe
Subject: Thank you for scheduling your online payment

CHASE

Dear JOHN DOE,

Thank you for scheduling your recent credit card payment online. Your payment will post to your account on 09/18/2006.

Now that you're making your payment online, are you aware of all the convenient ways you can manage your account online?

Just log in to www.chase.com today. Using the "I'd like to..." links for your credit card account, you can access more than a dozen features, including links to:

- **See Statements** - View your statement and choose to stop receiving paper statements.
- **Manage automatic payments** - Set up monthly payments to be made automatically.
- **Transfer a balance** - Transfer a balance to your credit card account.
- **Go to Free Alerts** - Schedule alerts to be reminded of key account activity.

You can also view past payments you have made online by logging on to www.chase.com and clicking "See payment history" under "I'd like to ..." .

If you have any problems or questions, please call the Customer Service number on the back of your credit card.

Thanks again for using online payments.

Sincerely,
Cardmember Services

This email was sent to: johndoe1972@gmail.com

(a)

Thank you for scheduling your online payment - Western European (ISO)
File Edit View Tools Message Help
Reply Reply All Forward Print Delete Previous Next Addresses

From: Chase Card Services
Date: Monday, September 18, 2006 12:25 PM
To: John Doe
Subject: Thank you for scheduling your online payment

CHASE JPMorgan

Dear JOHN DOE,

Thank you for scheduling your recent credit card payment online. Your payment will post to your account on 09/18/2006.

Now that you're making your payment online, are you aware of all the convenient ways you can manage your account online?

Just log in to www.chase.com today. Using the "I'd like to..." links for your credit card account, you can access more than a dozen features, including links to:

- **See Statements** - View your statement and choose to stop receiving paper statements.
- **Manage automatic payments** - Set up monthly payments to be made automatically.
- **Transfer a balance** - Transfer a balance to your credit card account.
- **Go to Free Alerts** - Schedule alerts to be reminded of key account activity.

You can also view past payments you have made online by logging on to www.chase.com and clicking "See payment history" under "I'd like to ..." .

If you have any problems or questions, please call the Customer Service number on the back of your credit card.

Thanks again for using online payments.

Sincerely,
Cardmember Services

Privacy | Terms of Use
© 2006 JPMorgan Chase & Co.

This email was sent to: johndoe1972@gmail.com

(b)

FIGURE e49.2 (a) Plain layout. (b) fancy layout.

Security Zone box, and a small-print footer filled with trademark, copyright, and contact notices as well as various informational and administrative hyperlinks. The principal login hyperlink conceals its destination. The test pair consists of the original message and a modified version that excludes the small print footer.

Weak Phishing Message

The sidebar "Phishing Message" shows a phishing message promising $50 for opening an account with Citibank. There is a simple company logo in the header; a footer contains legal disclaimers about the offer. There is no personalization, and the lone hyperlink is a made-up domain (actually owned by an unrelated organization), http://www.citibank.switch-today.com. Figure e49.5 contains its screenshot. The two versions differ only by the presence of a center-aligned "VeriSign Secured" endorsement logo that follows the footer's legal disclaimers.

Authentic Message

The test determines the impact of a "VeriSign Secured" logo added to the footer of an authentic message, as shown in Figure e49.6. The notice begins with a personalized greeting and informs the client about changes in PayPal's logo insertion policy. The message body is considerably longer than all of the other messages except for

Phishing Message

Dear Online Banker,

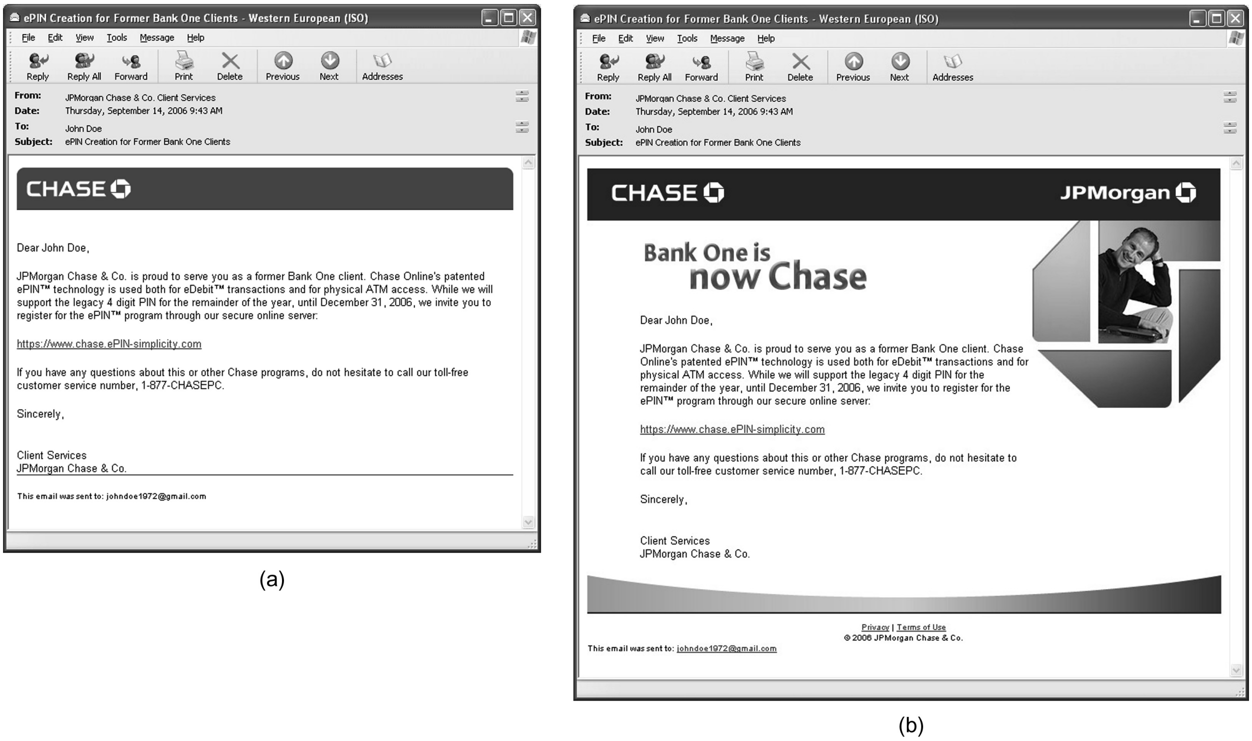
Citibank has recently upgraded its online banking service to provide best-in-industry safety, security and overall better experience. We're so excited about it, we'll pay you $50* to try it out! For a limited time if you open a FREE account with Citibank and deposit at least $100, we'll credit $50 to your account. It's our way of saying "Thanks for banking with us!"

This offer is only valid for a limited time.

Go to http://www.citibank.switch-today.com to start! We look forward to serving you.

Best Regards,
Citibank Web Services

*. Offer valid for a limited time only. Account must be opened with $100 minimum deposit made by ACH transfer. Account must remain open for at least six months or an early closing penalty will be assessed. See website for full terms and conditions.


ePIN Creation for Former Bank One Clients - Western European (ISO)
File Edit View Tools Message Help
Reply Reply All Forward Print Delete Previous Next Addresses

From: JPMorgan Chase & Co. Client Services
Date: Thursday, September 14, 2006 9:43 AM
To: John Doe
Subject: ePIN Creation for Former Bank One Clients

Dear John Doe,

JPMorgan Chase & Co. is proud to serve you as a former Bank One client. Chase Online's patented ePIN™ technology is used both for eDebit™ transactions and for physical ATM access. While we will support the legacy 4 digit PIN for the remainder of the year, until December 31, 2006, we invite you to register for the ePIN™ program through our secure online server:

https://www.chase.ePIN-simplicity.com

If you have any questions about this or other Chase programs, do not hesitate to call our toll-free customer service number, 1-877-CHASEPC.

Sincerely,

Client Services
JPMorgan Chase & Co.

This email was sent to: johndoe1972@gmail.com

(a)

ePIN Creation for Former Bank One Clients - Western European (ISO)
File Edit View Tools Message Help
Reply Reply All Forward Print Delete Previous Next Addresses

From: JPMorgan Chase & Co. Client Services
Date: Thursday, September 14, 2006 9:43 AM
To: John Doe
Subject: ePIN Creation for Former Bank One Clients

Dear John Doe,

JPMorgan Chase & Co. is proud to serve you as a former Bank One client. Chase Online's patented ePIN™ technology is used both for eDebit™ transactions and for physical ATM access. While we will support the legacy 4 digit PIN for the remainder of the year, until December 31, 2006, we invite you to register for the ePIN™ program through our secure online server:

https://www.chase.ePIN-simplicity.com

If you have any questions about this or other Chase programs, do not hesitate to call our toll-free customer service number, 1-877-CHASEPC.

Sincerely,

Client Services
JPMorgan Chase & Co.

Privacy | Terms of Use
© 2006 JPMorgan Chase & Co.

This email was sent to: johndoe1972@gmail.com

(b)

FIGURE e49.3 (a) Using a plain layout schema (b) using a fancy layout schema; and (c) using a plain and fancy layout schema.

the Netflix stimulus. The primary message contains no hyperlinks, but their small-print footer furnishes a hyperlink to unsubscribe from their newsletter. One interesting feature of the message is a boldfaced statement: "If you do not wish to have PayPal automatically inserted in your listings, you must update your preferences by 9/25." Though genuine, this message parallels the account shutdown threats brandished by many phishing messages. The header contains a monochrome company logo and a two-tone horizontal separation bar.

Login Page

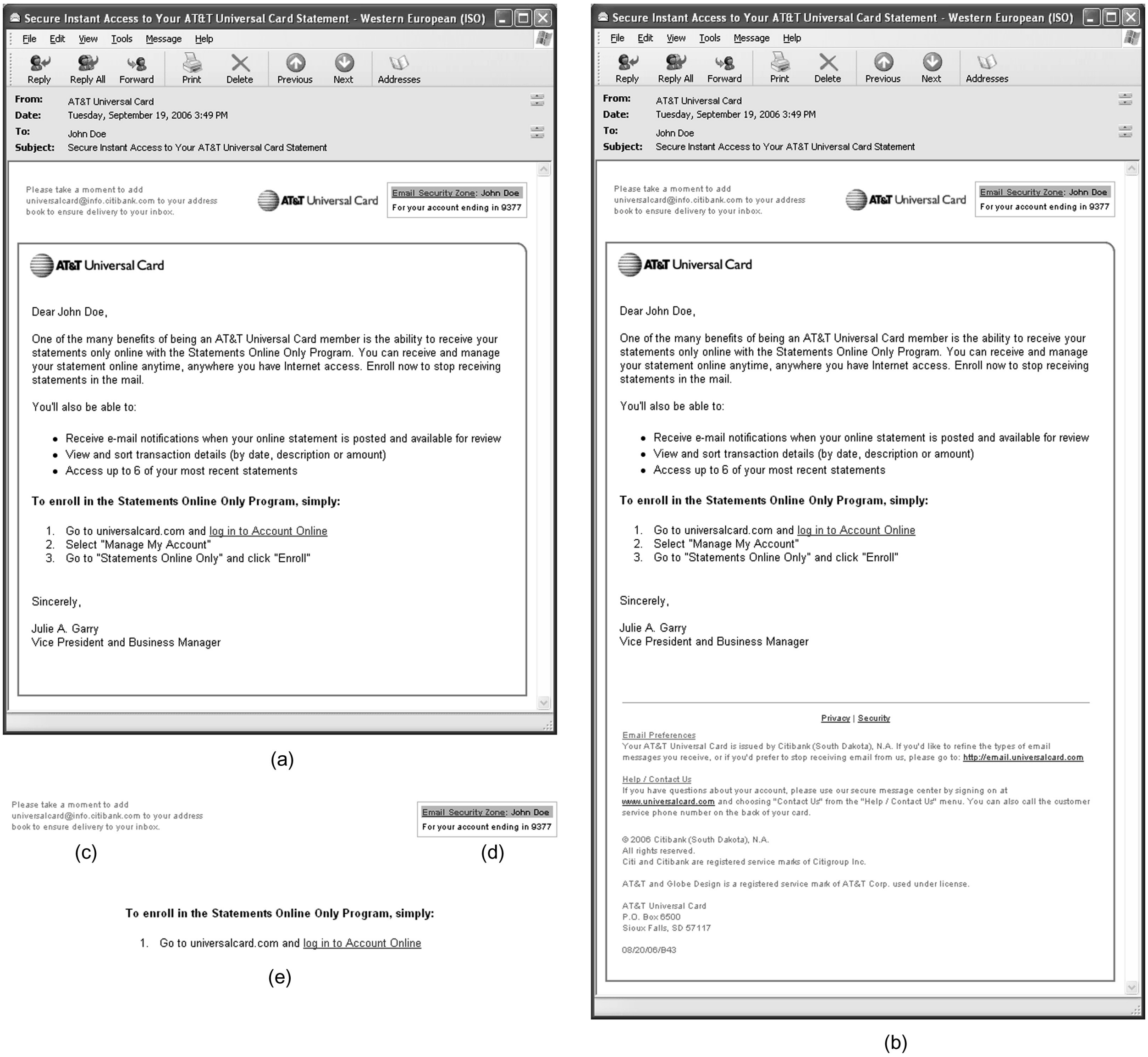
We say that the URL is strongly aligned with the content of the page when these two "belong together." Imagine that one would look at some ten Web pages (without associated URLs), and then some ten randomly ordered URLs, each one belonging to one of the ten Web pages. The easier it is for a potential reader to correctly pair up Web pages and URLs, the stronger the alignment. If any Web page and associated URL is not correctly matched up, then the alignment is very weak.

Let's now turn to an example, as shown in Figure e49.7. This browser's content window displays an exact copy of the AT&T Universal card login page. Like most Web login pages, it displays a high level of layout sophistication: photographs of happy clients, navigation bars, product pictures, a sidebar, promotional windows, and small-print legal disclaimers. It also displays a "VeriSign Secured" site endorsement logo. The two versions of this stimulus differ by their address bar contents: version (a) uses https://www.accountonline.com/View?docId = Index&siteId = AC&langId = EN and consequently displays a browser frame padlock; version (b) uses the unencrypted URL http://www.attuniversalcard.com/ (owned by AT&T but not in use).

Login Page: Strong and Weak Content Alignment

This next set takes the alternative approach to aligning the address bar URL with content: change the content. Both pages (see Figure e49.8) use the unregistered URL www.citicardmembers.com/. Version (a) displays a precise copy of the authentic Citi Credit Cards login page in its content window, whereas the version (b) content window displays modified logos and links (see Figure e49.9) for better alignment with the URL.

Figures 49.8a and 49.8b use a sophisticated layout with nearly all the same identifiable features of the AT&T Universal Card login: photographs of happy clients, navigation bars, product pictures, sidebars, promotional windows, and the "VeriSign Secured" logo.



From: AT&T Universal Card
Date: Tuesday, September 19, 2006 3:49 PM
To: John Doe
Subject: Secure Instant Access to Your AT&T Universal Card Statement

Please take a moment to add
universalcard@info.citibank.com to your address
book to ensure delivery to your inbox.

Email Security Zone: John Doe
For your account ending in 9377

Dear John Doe,

One of the many benefits of being an AT&T Universal Card member is the ability to receive your statements only online with the Statements Online Only Program. You can receive and manage your statement online anytime, anywhere you have Internet access. Enroll now to stop receiving statements in the mail.

You'll also be able to:

- Receive e-mail notifications when your online statement is posted and available for review
- View and sort transaction details (by date, description or amount)
- Access up to 6 of your most recent statements

To enroll in the Statements Online Only Program, simply:

1. Go to universalcard.com and log in to Account Online
2. Select "Manage My Account"
3. Go to "Statements Online Only" and click "Enroll"

Sincerely,

Julie A. Garry
Vice President and Business Manager

(a)

Please take a moment to add
universalcard@info.citibank.com to your address
book to ensure delivery to your inbox.

(c)

Email Security Zone: John Doe
For your account ending in 9377

(d)

To enroll in the Statements Online Only Program, simply:

1. Go to universalcard.com and log in to Account Online

(e)

From: AT&T Universal Card
Date: Tuesday, September 19, 2006 3:49 PM
To: John Doe
Subject: Secure Instant Access to Your AT&T Universal Card Statement

Please take a moment to add
universalcard@info.citibank.com to your address
book to ensure delivery to your inbox.

Email Security Zone: John Doe
For your account ending in 9377

Dear John Doe,

One of the many benefits of being an AT&T Universal Card member is the ability to receive your statements only online with the Statements Online Only Program. You can receive and manage your statement online anytime, anywhere you have Internet access. Enroll now to stop receiving statements in the mail.

You'll also be able to:

- Receive e-mail notifications when your online statement is posted and available for review
- View and sort transaction details (by date, description or amount)
- Access up to 6 of your most recent statements

To enroll in the Statements Online Only Program, simply:

1. Go to universalcard.com and log in to Account Online
2. Select "Manage My Account"
3. Go to "Statements Online Only" and click "Enroll"

Sincerely,

Julie A. Garry
Vice President and Business Manager

Privacy | Security

Email Preferences
Your AT&T Universal Card is issued by Citibank (South Dakota), N.A. If you'd like to refine the types of email messages you receive, or if you'd prefer to stop receiving email from us, please go to: http://email.universalcard.com

Help / Contact Us
If you have questions about your account, please use our secure message center by signing on at www.universalcard.com and choosing "Contact Us" from the "Help / Contact Us" menu. You can also call the customer service phone number on the back of your card.

© 2006 Citibank (South Dakota), N.A.
All rights reserved.
Citi and Citibank are registered service marks of Citigroup Inc.

AT&T and Globe Design is a registered service mark of AT&T Corp. used under license.

AT&T Universal Card
P.O. Box 6500
Sioux Falls, SD 57117

08/20/06/B43

(b)

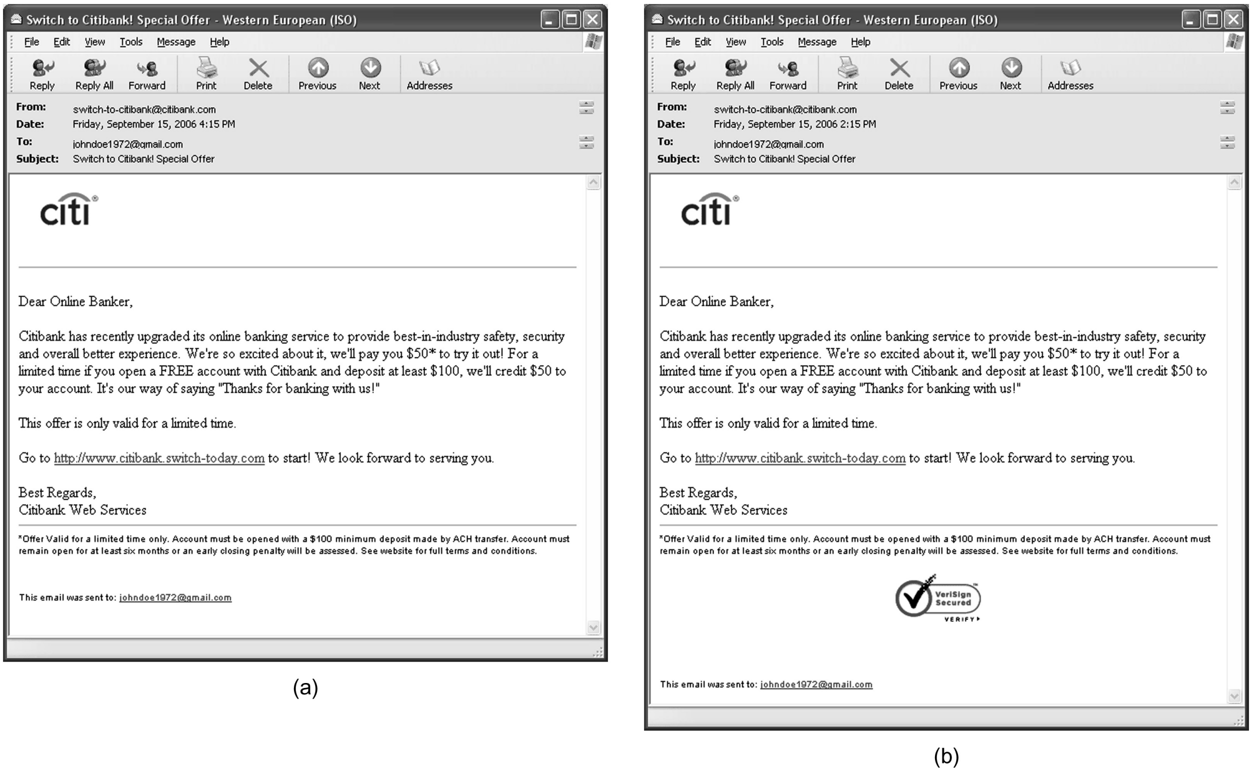
FIGURE e49.4 (a) An authentic message from the AT&T Universal card that promotes the company's paperless billing system. (b) an authentic message from AT&T Universal card that personalizes the greeting and includes the last four digits of the account number; (c) header detail left side; (d) header detail right side; and (e) hyperlink detail.

Login Page: Authentic and Bogus (But Plausible) URLs

These two stimuli test the impact of changing a well-aligned authentic URL (see Figure e49.9), http://www.paypal.com/ebay, to a reasonably well-aligned bogus URL, http://www.ebaygroup.com/paypal (domain owned by eBay but not in use). The main content window is the same for both: The eBay decorated version of the PayPal login page, which contains an eBay logo to the lower right of the primary PayPal logo. The page layout contains all the main features of the previous login pages but includes a more thorough set of third-party endorsement logos: "VeriSign Secured," "Reviewed by TRUST-e," and "Privacy: BBB OnLine." SSL is not used in either stimulus.

Login Page: Hard and Soft Emphasis on Security

Figure e49.10 tests whether it is possible to undermine confidence in an authentic login page with excessive concern about security and online fraud. These two stimuli represent an extreme but real-world case. Clients of the


Switch to Citibank! Special Offer - Western European (ISO)
File Edit View Tools Message Help
Reply
Reply All
Forward
Print
Delete
Previous
Next
Addresses
citi
VeriSign Secured
VERIFY
(a)
(b)

From: switch-to-citibank@citibank.com
Date: Friday, September 15, 2006 4:15 PM
To: johndoe1972@gmail.com
Subject: Switch to Citibank! Special Offer

Dear Online Banker,

Citibank has recently upgraded its online banking service to provide best-in-industry safety, security and overall better experience. We're so excited about it, we'll pay you $50* to try it out! For a limited time if you open a FREE account with Citibank and deposit at least $100, we'll credit $50 to your account. It's our way of saying "Thanks for banking with us!"

This offer is only valid for a limited time.

Go to http://www.citibank.switch-today.com to start! We look forward to serving you.

Best Regards,
Citibank Web Services

*Offer Valid for a limited time only. Account must be opened with a $100 minimum deposit made by ACH transfer. Account must remain open for at least six months or an early closing penalty will be assessed. See website for full terms and conditions.

This email was sent to: johndoe1972@gmail.com

From: switch-to-citibank@citibank.com
Date: Friday, September 15, 2006 2:15 PM
To: johndoe1972@gmail.com
Subject: Switch to Citibank! Special Offer

Dear Online Banker,

Citibank has recently upgraded its online banking service to provide best-in-industry safety, security and overall better experience. We're so excited about it, we'll pay you $50* to try it out! For a limited time if you open a FREE account with Citibank and deposit at least $100, we'll credit $50 to your account. It's our way of saying "Thanks for banking with us!"

This offer is only valid for a limited time.

Go to http://www.citibank.switch-today.com to start! We look forward to serving you.

Best Regards,
Citibank Web Services

*Offer Valid for a limited time only. Account must be opened with a $100 minimum deposit made by ACH transfer. Account must remain open for at least six months or an early closing penalty will be assessed. See website for full terms and conditions.

This email was sent to: johndoe1972@gmail.com

FIGURE e49.5 (a) Effect of endorsement logo. (b) center-aligned "VeriSign Secured" endorsement logo.

Indiana University Employees Federal Credit Union (IUCU) were targeted by a phishing attack in early August 2006. In response, the credit union altered its Web page to include a large banner, as shown in Figure e49.10f.

They further augmented the news section with a similar message: "Warning! Phishing Scam in progress (learn more)." Finally, a section named "Critical Fraud Alerts" contained the exact same warning as the one from the news section. The twin page eliminates all phishing warnings (including the banner) and changes the "Critical Fraud Alerts" section heading to read "Fraud Prevention Center." Generally, the language was changed to sound "in control" rather than alarmist.

Bad URL, with and without SSL and Endorsement Logo

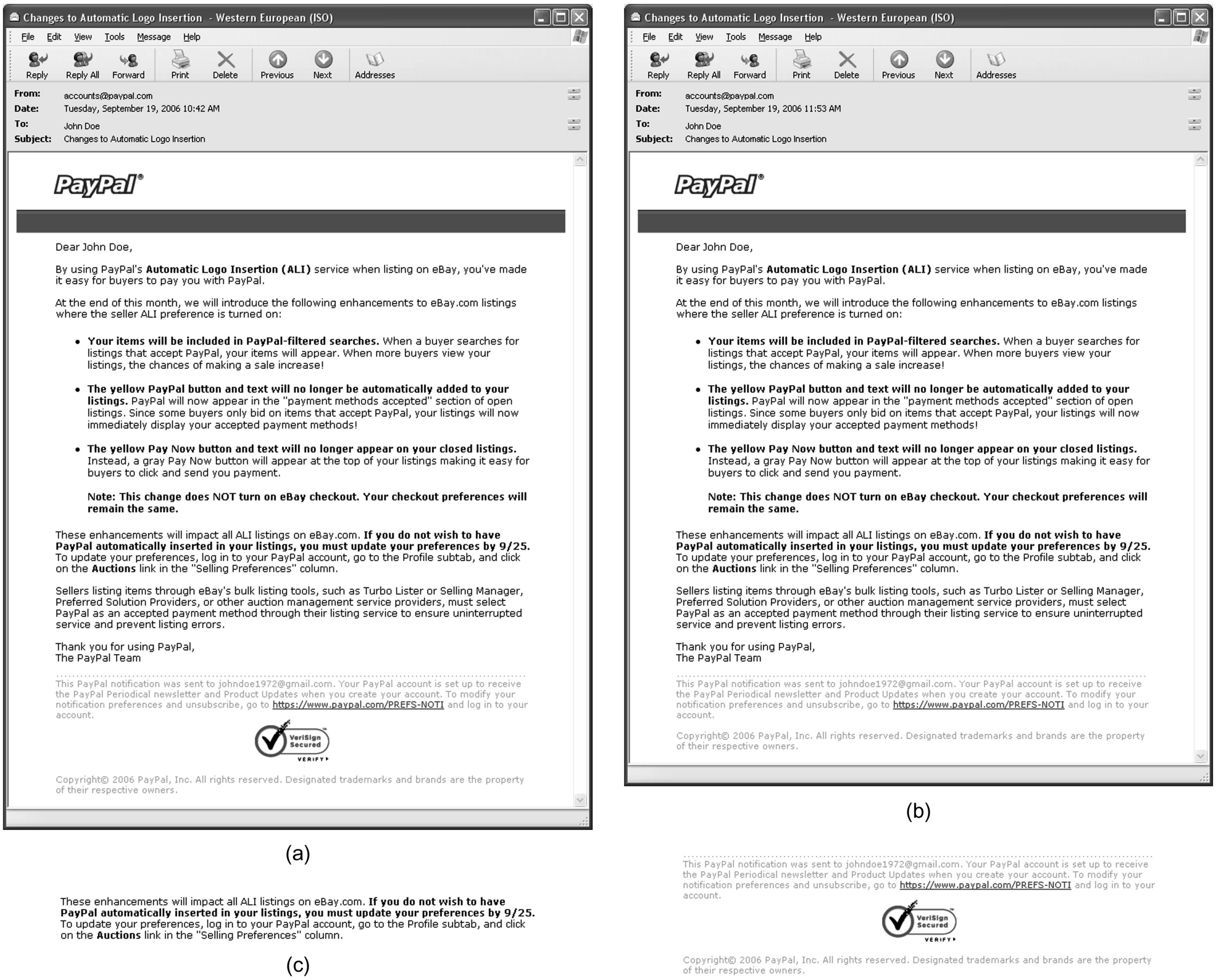
Can an endorsement logo and SSL padlock overcome a bad domain name? This next set, as shown in Figure e49.11, tests these two features on a Wells Fargo phishing site based on the bogus domain www-wellsfargo.com. The login page is similar in layout to the others but does not feature photographs of people. The only continuous tone graphic is an image of a speeding horse-drawn carriage that evokes a Wild West money transfer service. One screenshot contains the original page content using an unencrypted connection; the other stimulus uses SSL and adds a center-aligned "VeriSign Secured" logo to the page's footer.

High-Profile Recall Notice

At the time of testing (10/02/2006−10/12/2006), the press had been alive with recent reports[10] of laptop battery recalls from both Dell and Apple. Sony, the source of the batteries, ultimately issued a direct recall for the same batteries, by adding several more brands on 10/23/2006.

As shown in Figure e49.12, this test set does not follow the controlled-pair format of the previous stimuli. One stimulus is a screenshot of the official Dell Battery Return Program Web page. The page layout is substantially simpler than all other Web stimuli. A four-color header logo adorns the top of the page. It presents the content as a letter to "Dell Customer," explaining the danger and how to determine eligibility for exchange. Notably, there is a single column of content, no photos, and no promotional content of any kind. They use the third-party domain dellbatteryprogram.com. Use of this

[10] D. Darlin, "Dell will recall batteries in PCs," *New York Times*, 15 August 2006, http://select.nytimes.com/search/restricted/article?res = F10A1FF83C5A0C768DDDA10894DE404482.


Changes to Automatic Logo Insertion - Western European (ISO)
File Edit View Tools Message Help
Reply
Reply All
Forward
Print
Delete
Previous
Next
Addresses
PayPal®
VeriSign Secured
VERIFY

From: accounts@paypal.com
Date: Tuesday, September 19, 2006 10:42 AM
To: John Doe
Subject: Changes to Automatic Logo Insertion

Dear John Doe,

By using PayPal's **Automatic Logo Insertion (ALI)** service when listing on eBay, you've made it easy for buyers to pay you with PayPal.

At the end of this month, we will introduce the following enhancements to eBay.com listings where the seller ALI preference is turned on:

- **Your items will be included in PayPal-filtered searches.** When a buyer searches for listings that accept PayPal, your items will appear. When more buyers view your listings, the chances of making a sale increase!
- **The yellow PayPal button and text will no longer be automatically added to your listings.** PayPal will now appear in the "payment methods accepted" section of open listings. Since some buyers only bid on items that accept PayPal, your listings will now immediately display your accepted payment methods!
- **The yellow Pay Now button and text will no longer appear on your closed listings.** Instead, a gray Pay Now button will appear at the top of your listings making it easy for buyers to click and send you payment.

  Note: This change does NOT turn on eBay checkout. Your checkout preferences will remain the same.

These enhancements will impact all ALI listings on eBay.com. **If you do not wish to have PayPal automatically inserted in your listings, you must update your preferences by 9/25.** To update your preferences, log in to your PayPal account, go to the Profile subtab, and click on the **Auctions** link in the "Selling Preferences" column.

Sellers listing items through eBay's bulk listing tools, such as Turbo Lister or Selling Manager, Preferred Solution Providers, or other auction management service providers, must select PayPal as an accepted payment method through their listing service to ensure uninterrupted service and prevent listing errors.

Thank you for using PayPal,
The PayPal Team

This PayPal notification was sent to johndoe1972@gmail.com. Your PayPal account is set up to receive the PayPal Periodical newsletter and Product Updates when you create your account. To modify your notification preferences and unsubscribe, go to https://www.paypal.com/PREFS-NOTI and log in to your account.

Copyright© 2006 PayPal, Inc. All rights reserved. Designated trademarks and brands are the property of their respective owners.

(a)

From: accounts@paypal.com
Date: Tuesday, September 19, 2006 11:53 AM
To: John Doe
Subject: Changes to Automatic Logo Insertion

Dear John Doe,

By using PayPal's **Automatic Logo Insertion (ALI)** service when listing on eBay, you've made it easy for buyers to pay you with PayPal.

At the end of this month, we will introduce the following enhancements to eBay.com listings where the seller ALI preference is turned on:

- **Your items will be included in PayPal-filtered searches.** When a buyer searches for listings that accept PayPal, your items will appear. When more buyers view your listings, the chances of making a sale increase!
- **The yellow PayPal button and text will no longer be automatically added to your listings.** PayPal will now appear in the "payment methods accepted" section of open listings. Since some buyers only bid on items that accept PayPal, your listings will now immediately display your accepted payment methods!
- **The yellow Pay Now button and text will no longer appear on your closed listings.** Instead, a gray Pay Now button will appear at the top of your listings making it easy for buyers to click and send you payment.

  Note: This change does NOT turn on eBay checkout. Your checkout preferences will remain the same.

These enhancements will impact all ALI listings on eBay.com. **If you do not wish to have PayPal automatically inserted in your listings, you must update your preferences by 9/25.** To update your preferences, log in to your PayPal account, go to the Profile subtab, and click on the **Auctions** link in the "Selling Preferences" column.

Sellers listing items through eBay's bulk listing tools, such as Turbo Lister or Selling Manager, Preferred Solution Providers, or other auction management service providers, must select PayPal as an accepted payment method through their listing service to ensure uninterrupted service and prevent listing errors.

Thank you for using PayPal,
The PayPal Team

This PayPal notification was sent to johndoe1972@gmail.com. Your PayPal account is set up to receive the PayPal Periodical newsletter and Product Updates when you create your account. To modify your notification preferences and unsubscribe, go to https://www.paypal.com/PREFS-NOTI and log in to your account.

Copyright© 2006 PayPal, Inc. All rights reserved. Designated trademarks and brands are the property of their respective owners.

(b)

These enhancements will impact all ALI listings on eBay.com. **If you do not wish to have PayPal automatically inserted in your listings, you must update your preferences by 9/25.** To update your preferences, log in to your PayPal account, go to the Profile subtab, and click on the **Auctions** link in the "Selling Preferences" column.

(c)

This PayPal notification was sent to johndoe1972@gmail.com. Your PayPal account is set up to receive the PayPal Periodical newsletter and Product Updates when you create your account. To modify your notification preferences and unsubscribe, go to https://www.paypal.com/PREFS-NOTI and log in to your account.

Copyright© 2006 PayPal, Inc. All rights reserved. Designated trademarks and brands are the property of their respective owners.

(d)

FIGURE e49.6 (a) "VeriSign Secured" logo added to the footer of an authentic message. (b) authentic message—effect of endorsement logo; (c) shared body detail; (d) endorsement footer detail.

domain for the official page makes the replacement service ripe for phishing.

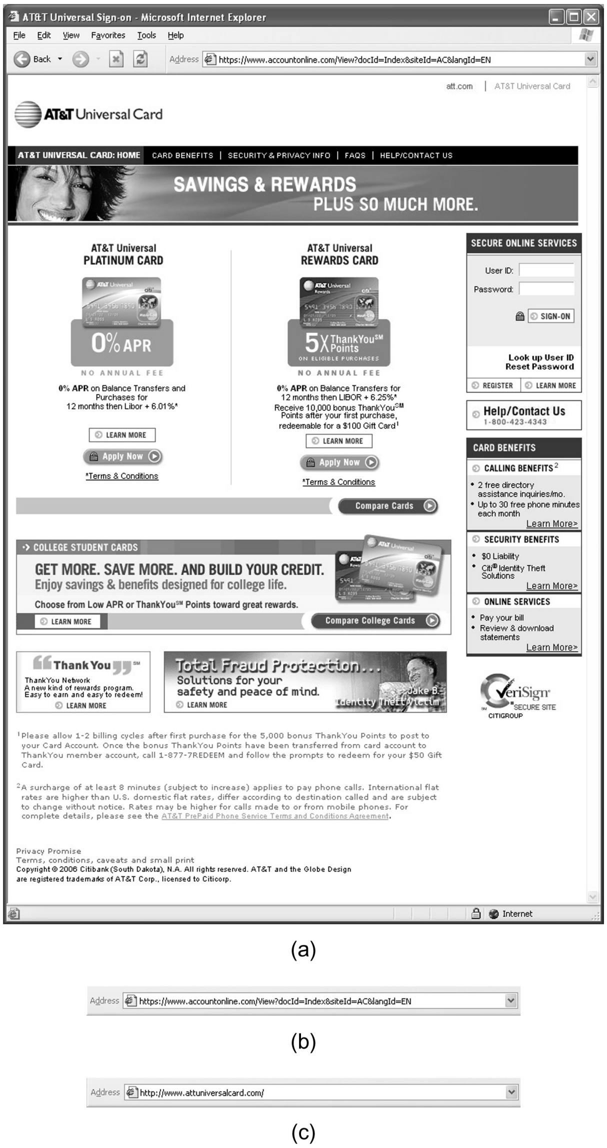
We constructed a phishing email message using the header, footer, and textual content from this Web page. The phishing message omits the middle section on how to identify eligible batteries and instead requests that the recipient go to the bogus Web page at http://www.dellbatteryreplacements.com.

Low-Profile Class-Action Lawsuit

As shown in Figure e49.13, this last set of stimuli also follows the third-party email and Web page form of the previous set. Both stimuli are authentic, but they use altered dates to appear relevant at the time of testing. The email message is a lengthy notice that describes a class-action lawsuit against Netflix, a settlement to the lawsuit, and options for claiming benefits. There is no greeting, signature, color, or graphics. The only hyperlinks direct the user to the authentic third-party URL, http://www.netflixsettlement.com. The Web page has a similarly bare appearance but with much less text. It behaves as a hyperlink gateway for more information under the URL http://www.netflix.com/settlement/ (the result of redirection from http://www.netflixsettlement.com).

2. RESULTS AND ANALYSIS

Our experiment directly controls for the effect of several design features. There are some surprises in the direct results from these tests, including the stunning impact of a detailed small print footer on an otherwise well-conceived legitimate message; however, the experiment reveals an unexpected, but in retrospect obvious, lesson



0% APR on Balance Transfers and Purchases for 12 months then Libor + 6.01%*

0% APR on Balance Transfers for 12 months then LIBOR + 6.25%* Receive 10,000 bonus ThankYou^{SM} Points after your first purchase, redeemable for a $100 Gift Card[1]

- 2 free directory assistance inquiries/mo.
- Up to 30 free phone minutes each month

- $0 Liability
- Citi® Identity Theft Solutions

- Pay your bill
- Review & download statements

GET MORE. SAVE MORE. AND BUILD YOUR CREDIT.
Enjoy savings & benefits designed for college life.
Choose from Low APR or ThankYou^{SM} Points toward great rewards.

ThankYou Network
A new kind of rewards program.
Easy to earn and easy to redeem!

Solutions for your safety and peace of mind.

[1]Please allow 1-2 billing cycles after first purchase for the 5,000 bonus ThankYou Points to post to your Card Account. Once the bonus ThankYou Points have been transferred from card account to ThankYou member account, call 1-877-7REDEEM and follow the prompts to redeem for your $50 Gift Card.

[2]A surcharge of at least 8 minutes (subject to increase) applies to pay phone calls. International flat rates are higher than U.S. domestic flat rates, differ according to destination called and are subject to change without notice. Rates may be higher for calls made to or from mobile phones. For complete details, please see the AT&T PrePaid Phone Service Terms and Conditions Agreement.

Privacy Promise
Terms, conditions, caveats and small print
Copyright © 2006 Citibank (South Dakota), N.A. All rights reserved. AT&T and the Globe Design are registered trademarks of AT&T Corp., licensed to Citicorp.

(a)

Address https://www.accountonline.com/View?docId=Index&siteId=AC&langId=EN

(b)

Address http://www.attuniversalcard.com/

(c)

FIGURE e49.7 (a) Strong and weak URL alignment; (b) weak alignment URL detail; (c) strong alignment URL detail.

about email messages: The "story" of the message is critical. Messages with strong and succinct narrative components rated highly and their ratings appear to be less susceptible to changes in graphic design. On the other hand, authenticity perception changed significantly for messages that say little (such as a service promotion) under document feature variances. Two of the five sets of "twins" did not change significantly, according to the metric, when augmented with the very same features that produced significant changes in other messages. Subjects judged these messages principally on their narrative content.

The Chase phishing message uses the company's recent acquisition of Bank One as a pretext for imminent service change to ATM card authentication; the story further bundles this change with the addition of a new service, eDebit, and implicitly threatens discontinuation of service by claiming to "support the legacy 4 digit PIN for the remainder of the year." This consequence is much less direct than the standard "Your account will be suspended in 48 hours if ..." strategy used by many phishers. It works on a less urgent time scale and is pitched as a convenience to all clients rather than an anomaly specialized to a specific client. There was no significant difference in subject evaluation between the plainly formatted version of this message with the monochrome corporate header and the one with several customized continuous tone graphics.

Yet these same graphics, minus the shiny "Bank One is now Chase" banner, produced a significant change ($p = 0{:}018$) in evaluations of Chase's authentic payment notice. The payment notice thanks the receiver for a recent online payment, then goes on to inform the user about features of their online account management interface. In terms of relevance, there is less potential impact on the user. Ignoring this message won't expose the client to any changes (good or bad). Assuming that the name and recent online interaction are correct, the message communicates little that would surprise the average client. So, in place of strong narrative components, the subject looks to formatting cues to further inform confidence. This message rated highly in its simple form and was pushed higher by the improved graphics. We attribute its initially high rating to its exclusion of hyperlinks, informative nature, and well-contextualized message.

Subject reactions to the presence of the "VeriSign Secured" logo differed dramatically between the two test messages. One message, a change of policy notice from PayPal, experienced no statistical difference in subject evaluations of its endorsed and unendorsed forms. The policy change notice shares several narrative features with the Chase phishing message: Both messages have a customized salutation, both inform users about an institution wide change (in this case, the particulars of their logo insertion policy), and both claim that inaction will result in a change of service. The PayPal message has no hyperlink in the message body but does contain a link in its small-font gray footer to manage user preferences; we think that this forecasts a potential phishing strategy.

The other message that tests the impact of the "VeriSign Secured" logo is a phishing message that exploits the Citibank brand. The experiment shows a statistically significant change in subject evaluations ($p = 0{:}047$) due to this single feature change. Of all the messages, this message makes the weakest connections to the receiver. It begins with a generic salutation. Worse, the first sentence promotes the goodness of their online service but fails to involve the receiver in any way. Not

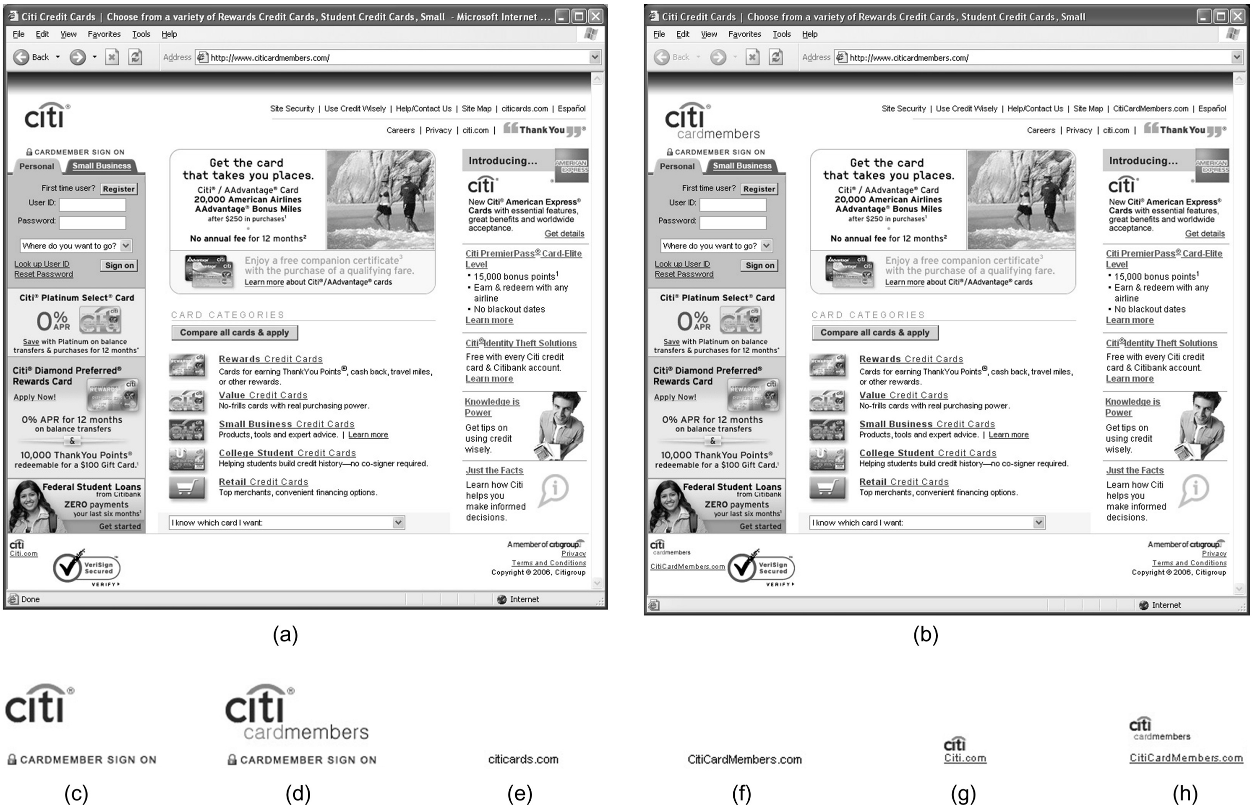


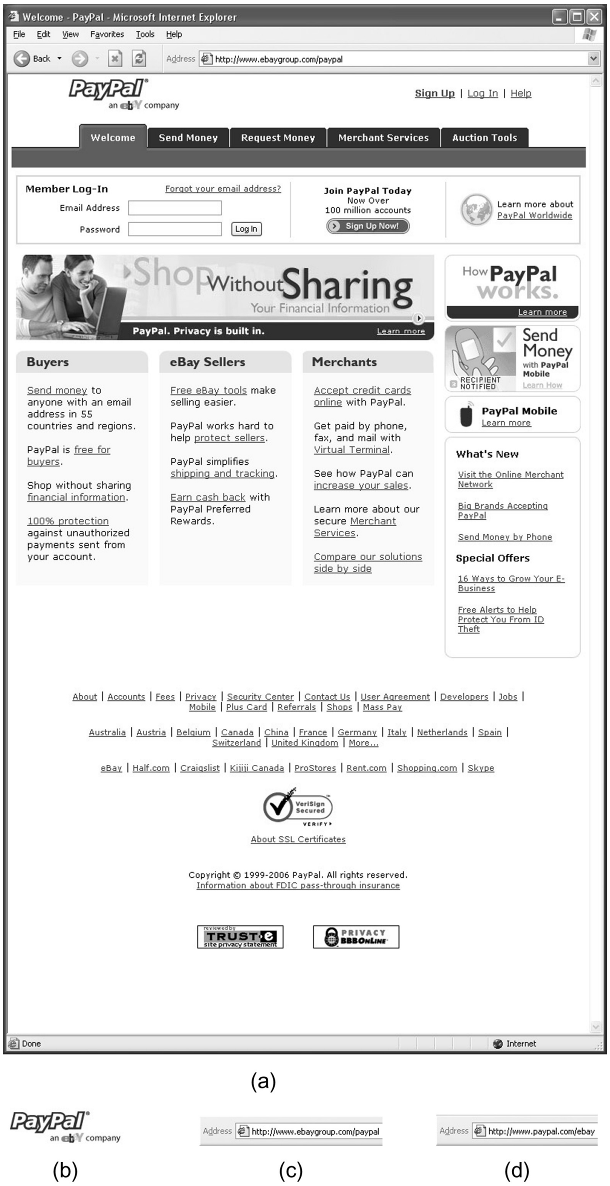
FIGURE e49.8 (a) A precise copy of the authentic Citi Credit Cards login page in its content window. (b) content window displays modified logos and links; (c) location of detail window; (d) original and modified detail window; (e) header menu of detail window; (f) Cardmember sign on detail window; (g) footer of detail window; and (h) Cardmembers of detail window.

until the second sentence does the message's relevance become evident to the reader: They are offering "$50* to try it out!" These two messages had the lowest average ranking of all the email stimuli. Ignoring this message has no impact on the user except for failing to miss out on an offer of dubious value. Ultimately, the stimulus fails to engage the reader, and so subjects base more of their evaluation on nonnarrative factors such as the endorsement logo and the bogus URL.

The Dell battery replacement program message presents a compelling story, but not directly. The incident received a high level of media coverage due to spectacular reports of exploding and burning laptop computers. The Dell message, which we manufactured, benefits from other sources spreading the story. Without this third-party validation, this message could have bordered on implausibility, but instead our subjects produced ratings that were statistically indistinguishable from the two most highly ranked email messages in the batch. This message contains a slightly nicer-than-average layout (multicolored header, footer graphic with links) but less personalization and a fraudulent (but semantically plausible) URL. The story was so powerful and present in the subjects' minds that they were willing to discount the suspicious link and generic greeting.

The other third-party attack (NetFlix) did not benefit from recent or high-profile media coverage (see Table e49.1). We may have further lowered its rating by altering the dates to appear relevant at the time of testing.

Subjects could have perceived the timeline as implausibly long (even for legal action) or may have been familiar with the case and known that the dates were incorrect. In addition to these changes, the original message is particularly poorly conceived. Though it has strong narrative elements that present lawsuit context, the elements of the settlement, and response options, the message is entirely too long. Message length and detail create an incentive for users to quickly evaluate according to nonnarrative features. The most visually obvious features are the inclusion of blue hyperlinks—the only non-black-and-white symbols—that point to http://www.netflixsettlement.com. Though this is the legitimate domain, it should raise suspicion because it is an apparent "cousin domain" to the parent company's Web site. The lack of strong design features seals its poor evaluation. There is no company header—a feature present on every other stimulus—and


Welcome - PayPal - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Address http://www.ebaygroup.com/paypal
PayPal an ebY company
Sign Up | Log In | Help
Welcome
Send Money
Request Money
Merchant Services
Auction Tools

Member Log-In Forgot your email address?
Email Address
Password Log In

Join PayPal Today
Now Over
100 million accounts
Sign Up Now!

Learn more about PayPal Worldwide

Shop Without Sharing Your Financial Information
PayPal. Privacy is built in. Learn more

How PayPal works. Learn more

Send Money with PayPal Mobile
RECIPIENT NOTIFIED
Learn How

PayPal Mobile
Learn more

Buyers

Send money to anyone with an email address in 55 countries and regions.

PayPal is free for buyers.

Shop without sharing financial information.

100% protection against unauthorized payments sent from your account.

eBay Sellers

Free eBay tools make selling easier.

PayPal works hard to help protect sellers.

PayPal simplifies shipping and tracking.

Earn cash back with PayPal Preferred Rewards.

Merchants

Accept credit cards online with PayPal.

Get paid by phone, fax, and mail with Virtual Terminal.

See how PayPal can increase your sales.

Learn more about our secure Merchant Services.

Compare our solutions side by side

What's New

Visit the Online Merchant Network

Big Brands Accepting PayPal

Send Money by Phone

Special Offers

16 Ways to Grow Your E-Business

Free Alerts to Help Protect You From ID Theft

About | Accounts | Fees | Privacy | Security Center | Contact Us | User Agreement | Developers | Jobs | Mobile | Plus Card | Referrals | Shops | Mass Pay

Australia | Austria | Belgium | Canada | China | France | Germany | Italy | Netherlands | Spain | Switzerland | United Kingdom | More...

eBay | Half.com | Craigslist | Kijiji Canada | ProStores | Rent.com | Shopping.com | Skype

VeriSign Secured VERIFY
About SSL Certificates

Copyright © 1999-2006 PayPal. All rights reserved.
Information about FDIC pass-through insurance

reviewed by TRUSTe site privacy statement
PRIVACY BBBOnLine

Done
Internet
(a)
PayPal an ebY company
Address http://www.ebaygroup.com/paypal
Address http://www.paypal.com/ebay
(b)
(c)
(d)

FIGURE e49.9 (a) A reasonably well-aligned bogus URL. (b) logo detail; (c) bogus URL detail; and (d) authentic URL detail.

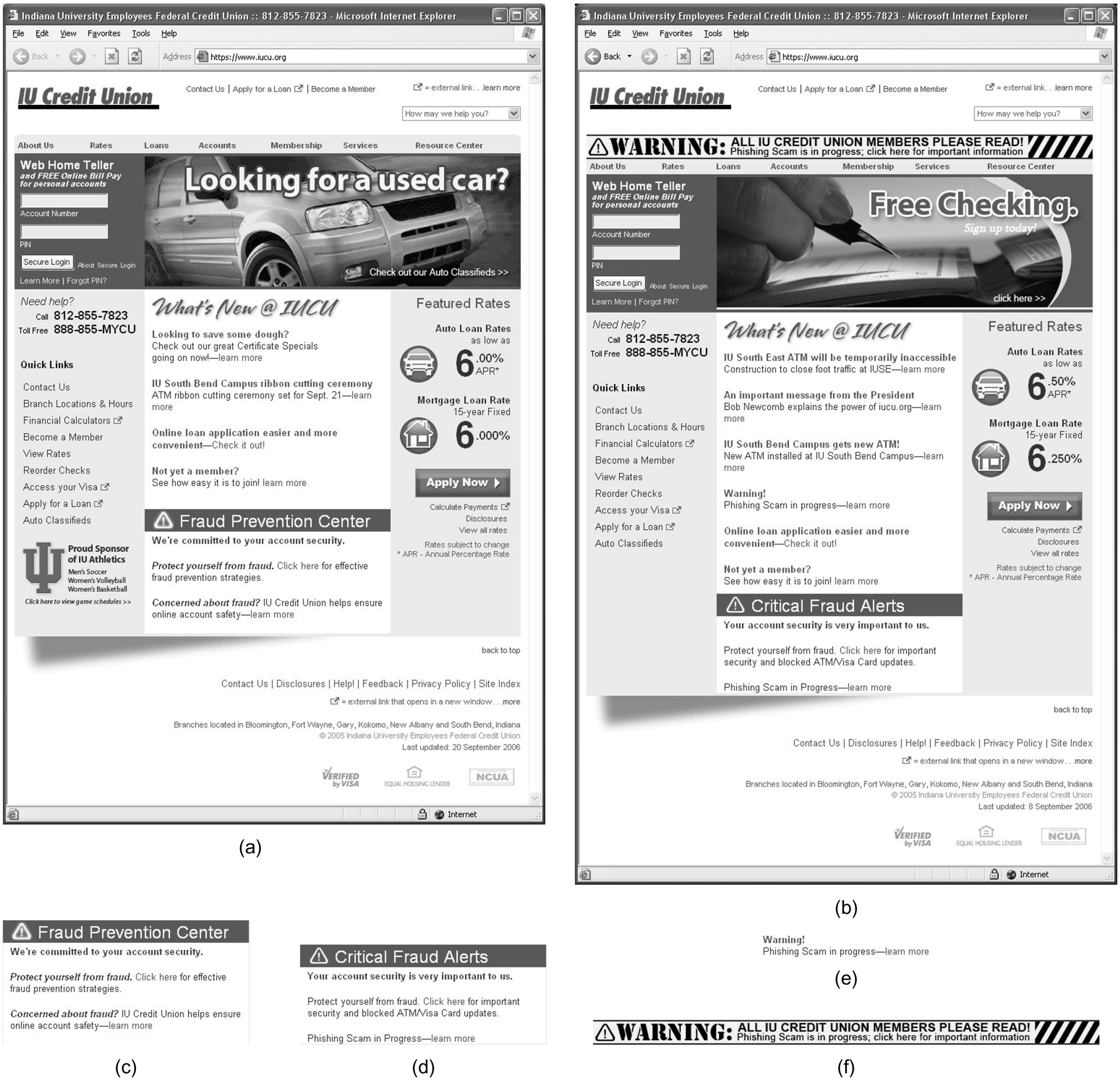
no opening salutation or signature. The contact address appears to be an afterthought that does not even specify a division of the company, let alone an appropriate administrator.

The biggest surprise of the test appears in a pair of authentic AT&T Universal card messages. In many ways, this is the polar opposite of the Netflix settlements message: it has strong design elements and a short, weak narrative. The message promotes AT&T's Statements Online Only program without bundling it with a recent action (as Chase does with its payment notification). Ignoring this message will not produce any change in the receiver's service, nor does enrolling in the program provide any obvious benefit to the client; in fact, enrollment could result in unintended late payments due to imperfect spam interdiction of electronic billing notices. What the message lacks in narrative appeal it makes up for in design strength. It customizes the message to the receiver both in the opening salutation and in an "Email Security Zone" header box that displays client name and client account number suffix. The header also has a spam awareness message and company logo. A blue outline that complements the company logo encloses the rest of the content. The corporate logo appears a second time within the blue content box and the letter opens and closes with personalized salutations: "Dear John Doe," and "Sincerely, Julie A. Garry." The two versions of this message differ in the presence of a detailed small-print footer below the signature, which contains hyperlinks to privacy and security policies, as well as hyperlinks bearing the universalcard.com domain. The footer uses a small gray font and presents text for adjusting "Email Preferences" and a "Help/Contact Us" section containing the postal address and various trademark and copyright notices.

The one ambiguous feature of this email is a centrally located hyperlink, labeled "log in to Account Online." It does not indicate the URL in the text. Phishers frequently employ this sort of hyperlinking strategy to conceal the bogus server's URL. The footer may add confidence because its hyperlinks appear to reference URLs with legitimate and semantically aligned domain names; none of the hyperlinks outside the header indicate a target domain. Alternatively, the contact, copyright, and trademark notices themselves may improve confidence in the message. It is particularly interesting that even though the footer-less message displayed the last four digits of the credit-card number, customized the greeting, and employed generally strong design elements, except for the Netflix settlement, it was still ranked lower than any other legitimate message. This supports the experimental results in[11] that indicate indifference to customized greetings in certain contexts. Yet adding the footer boosts the evaluations to the point where it is statistically indistinguishable from the other two most highly ranked messages—the Chase payment notification with fancy graphics and the Dell battery recall notice.

Web sites, particularly the login and information collection pages associated with phishing scams, do not present a story the way email messages do. For this reason, their credibility depends much more on document features and graphic design. Subjects assigned significantly

[11] M. Jakobsson and J. Ratkiewicz, "Designing ethical phishing experiments: a study of (rot13) ronl query features," In WWW *'06: Proceedings of the 15th International Conference on World Wide Web*, pp. 513–522, New York, 2006, ACM Press.


Indiana University Employees Federal Credit Union :: 812-855-7823 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Address https://www.iucu.org
IU Credit Union
Contact Us | Apply for a Loan | Become a Member
= external link. . .learn more
How may we help you?
About Us Rates Loans Accounts Membership Services Resource Center
Web Home Teller
and FREE Online Bill Pay for personal accounts
Account Number
PIN
Secure Login
About Secure Login
Learn More | Forgot PIN?
Looking for a used car?
Check out our Auto Classifieds >>
Need help?
Call 812-855-7823
Toll Free 888-855-MYCU
Quick Links
Contact Us
Branch Locations & Hours
Financial Calculators
Become a Member
View Rates
Reorder Checks
Access your Visa
Apply for a Loan
Auto Classifieds
Proud Sponsor of IU Athletics
Men's Soccer
Women's Volleyball
Women's Basketball
Click here to view game schedules >>
What's New @ IUCU
Featured Rates
Auto Loan Rates as low as
6.00% APR*
Mortgage Loan Rate 15-year Fixed
6.000%
Apply Now
Calculate Payments
Disclosures
View all rates
Rates subject to change
* APR - Annual Percentage Rate
back to top
Contact Us | Disclosures | Help! | Feedback | Privacy Policy | Site Index
= external link that opens in a new window. . .more
VERIFIED by VISA
EQUAL HOUSING LENDER
NCUA
Internet
(a)

Looking to save some dough?
Check out our great Certificate Specials going on now!—learn more

IU South Bend Campus ribbon cutting ceremony
ATM ribbon cutting ceremony set for Sept. 21—learn more

Online loan application easier and more convenient—Check it out!

Not yet a member?
See how easy it is to join! learn more

Fraud Prevention Center

We're committed to your account security.

Protect yourself from fraud. Click here for effective fraud prevention strategies.

Concerned about fraud? IU Credit Union helps ensure online account safety—learn more

Branches located in Bloomington, Fort Wayne, Gary, Kokomo, New Albany and South Bend, Indiana
© 2005 Indiana University Employees Federal Credit Union
Last updated: 20 September 2006

Indiana University Employees Federal Credit Union :: 812-855-7823 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Address https://www.iucu.org
IU Credit Union
Contact Us | Apply for a Loan | Become a Member
= external link. . .learn more
How may we help you?

WARNING: ALL IU CREDIT UNION MEMBERS PLEASE READ!
Phishing Scam is in progress; click here for important information

IU South East ATM will be temporarily inaccessible
Construction to close foot traffic at IUSE—learn more

An important message from the President
Bob Newcomb explains the power of iucu.org—learn more

IU South Bend Campus gets new ATM!
New ATM installed at IU South Bend Campus—learn more

Warning!
Phishing Scam in progress—learn more

Online loan application easier and more convenient—Check it out!

Not yet a member?
See how easy it is to join! learn more

Critical Fraud Alerts

Your account security is very important to us.

Protect yourself from fraud. Click here for important security and blocked ATM/Visa Card updates.

Phishing Scam in Progress—learn more

Branches located in Bloomington, Fort Wayne, Gary, Kokomo, New Albany and South Bend, Indiana
© 2005 Indiana University Employees Federal Credit Union
Last updated: 8 September 2006

Fraud Prevention Center

We're committed to your account security.

Protect yourself from fraud. Click here for effective fraud prevention strategies.

Concerned about fraud? IU Credit Union helps ensure online account safety—learn more

Critical Fraud Alerts

Your account security is very important to us.

Protect yourself from fraud. Click here for important security and blocked ATM/Visa Card updates.

Phishing Scam in Progress—learn more

Warning!
Phishing Scam in progress—learn more

WARNING: ALL IU CREDIT UNION MEMBERS PLEASE READ!
Phishing Scam is in progress; click here for important information

FIGURE e49.10 (a) Soft emphasis on security; (b) hard emphasis on security; (c) soft security detail; (d) hard security detail; (d) hard security detail 1; (e) soft security detail 2; and (f) Web page warning.

different ratings to three of the five sets of twin stimuli. The results show that address bar alignment with page content, overwrought concerns about fraud, and third-party endorsements substantively change authenticity assessments.

The biggest rating difference among the Web page stimuli was measured between the two versions of the "AT&T Universal Card Sign-on" page. The official version, which uses the address URL https://www.accounton-line.com/View?docId = Index&siteId = A C&langId = EN, has the lowest average rating of the ten Web stimuli in the paired testing. With an average rating of 2.76, it rated lower than a simulated phishing Web site based on the suspiciously formed domain www-wellsfargo.com (avg. rating: 3.17). Subjects who saw the unused domain http://www.attuniversalcard.com in the address bar of the AT&T card login page rated it significantly higher ($p = 0{:}004$) than the authentic page. The page content strongly aligns with the URL text http://www.attuniversalcard.com: the phrase "AT&T Universal" appears no less than seven times on the login page, whereas the phrase "AT&T Universal Card" appears four times in the content window. Interestingly, the official page uses HTTPS and displays an SSL padlock in the

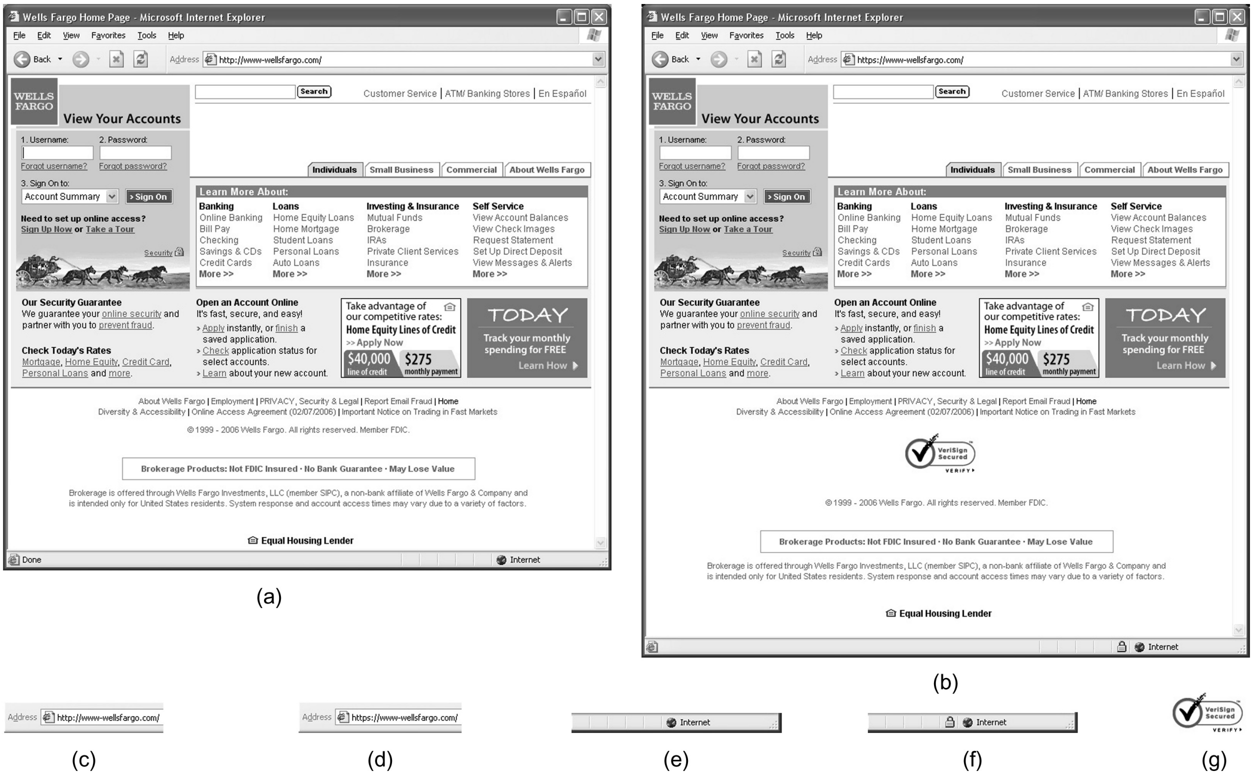

Wells Fargo Home Page - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Address http://www-wellsfargo.com/
Address https://www-wellsfargo.com/
WELLS FARGO
View Your Accounts
1. Username: 2. Password:
Forgot username? Forgot password?
3. Sign On to:
Account Summary
> Sign On
Need to set up online access?
Sign Up Now or Take a Tour
Security
Search
Customer Service | ATM/ Banking Stores | En Español
Individuals Small Business Commercial About Wells Fargo
Learn More About:
Banking
Online Banking
Bill Pay
Checking
Savings & CDs
Credit Cards
More >>
Loans
Home Equity Loans
Home Mortgage
Student Loans
Personal Loans
Auto Loans
More >>
Investing & Insurance
Mutual Funds
Brokerage
IRAs
Private Client Services
Insurance
More >>
Self Service
View Account Balances
View Check Images
Request Statement
Set Up Direct Deposit
View Messages & Alerts
More >>
Our Security Guarantee
We guarantee your online security and partner with you to prevent fraud.
Check Today's Rates
Mortgage, Home Equity, Credit Card, Personal Loans and more.
Open an Account Online
It's fast, secure, and easy!
> Apply instantly, or finish a saved application.
> Check application status for select accounts.
> Learn about your new account.
Take advantage of our competitive rates:
Home Equity Lines of Credit
>> Apply Now
$40,000 line of credit
$275 monthly payment
TODAY
Track your monthly spending for FREE
Learn How
About Wells Fargo | Employment | PRIVACY, Security & Legal | Report Email Fraud | Home
Diversity & Accessibility | Online Access Agreement (02/07/2006) | Important Notice on Trading in Fast Markets
© 1999 - 2006 Wells Fargo. All rights reserved. Member FDIC.
Brokerage Products: Not FDIC Insured · No Bank Guarantee · May Lose Value
Brokerage is offered through Wells Fargo Investments, LLC (member SIPC), a non-bank affiliate of Wells Fargo & Company and is intended only for United States residents. System response and account access times may vary due to a variety of factors.
Equal Housing Lender
VeriSign Secured VERIFY
Done
Internet
(a)
(b)
(c)
(d)
(e)
(f)
(g)

FIGURE e49.11 (a) Without SSL and endorsement logo. (b) with SSL and endorsement logo; (c) no SSL/endorsement logo; (d) SSL/endorsement detail; (e) Internet no SSL/endorsement status bar; (f) Internet SSL/endorsement status bar; and (g) VeriSign logo.

lower right-hand browser frame, whereas the attuniversalcard.com domain does not use SSL and consequently does not display the padlock on the browser frame. Subjects found the semantic alignment of the URL to be a much stronger indicator of authenticity than SSL utilization. In fairness, subjects could not examine the certificates, nor would they have been subject to the "Unable to verify the identity of host" pop-up window in the case of a self-signed certificate. Nevertheless, other user studies have found that in practice, subjects rarely consider these factors.[12,13]

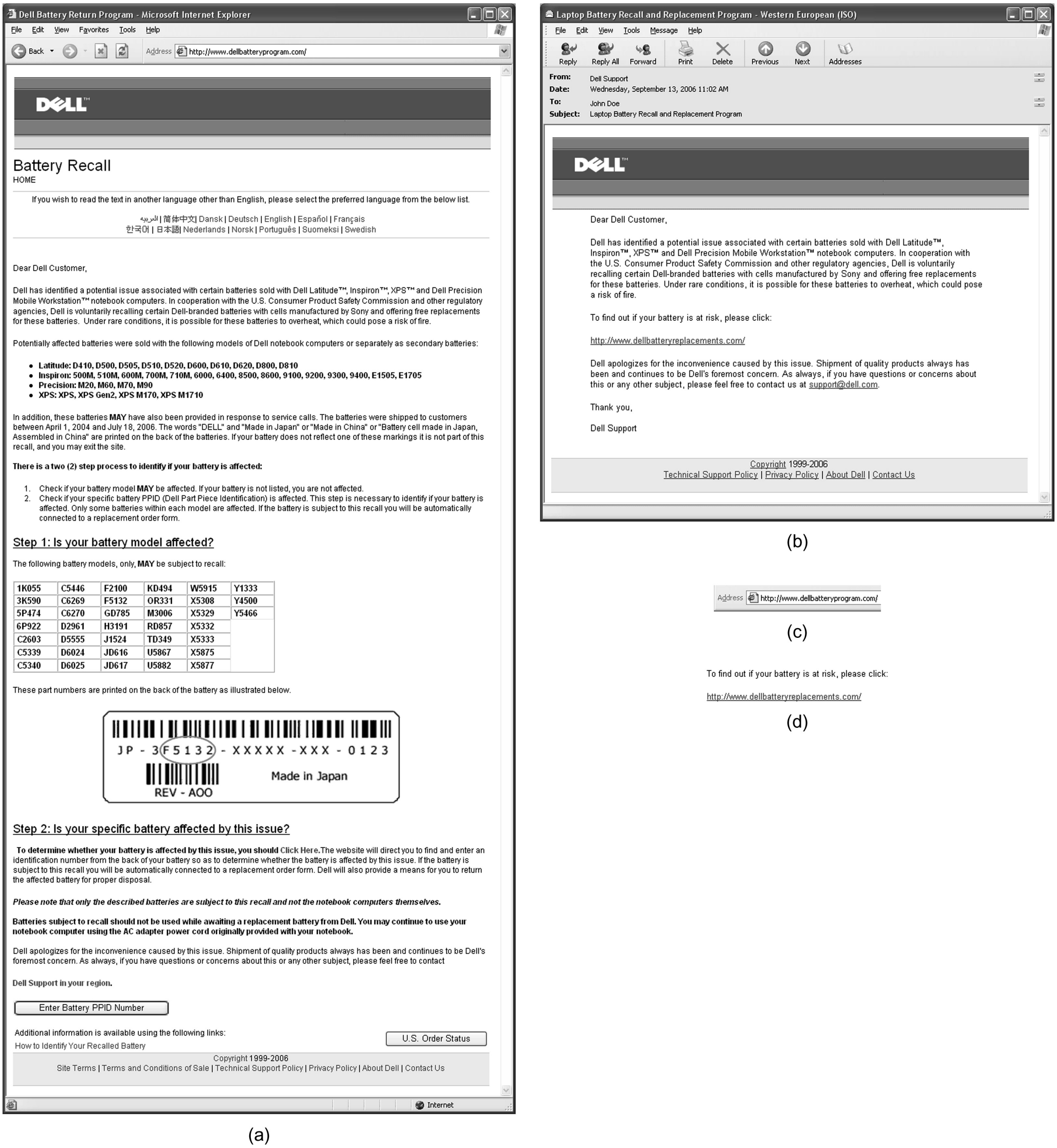
Much to our surprise, the phishing simulation based on the URL www-wellsfargo.com rated significantly higher ($p = 0{:}00001$) than the official AT&T Universal card login page. Subjects valued semantic alignment between content and host domain more than domain well-formedness. Syntactically there is nothing wrong with the domain, but replacing the dot with a dash is clearly an attempt at deception. Adding SSL and a "VeriSign Secured" logo to the Wells-Fargo phishing page produced a significant improvement in authenticity ratings ($p = 0{:}029$). It's worth noting that the authentic login page (not in the test) does not display a VeriSign logo but does use SSL. In spite of subjects either failing to notice the dash-for-dot exchange or not thinking that it was suspicious, they did notice the presence of either SSL or the VeriSign logo. Note that the AT&T login page also used SSL and displayed a VeriSign endorsement, but neither of these features could overcome the mistrust of the accountonline.com domain.

The last statistically significant difference between twins in the Indiana University Credit Union homepage ($p = 0{:}022$) shows that too much concern about security can reduce customer confidence. Subjects responded positively to use of less fearful language and rated the softer, more constructive content significantly higher than the page that displayed stark warnings. Note that correct domain names and SSL were used on both stimuli. This is a case where a good-faith effort to educate clients about phishing undermines confidence in the Web site's authenticity. Login pages are no place for fear-provoking messages.

One way phishers align page content with URLs is by choosing an apt domain name; the other way is to change

[12] R. Dhamija, J. D. Tygar, and M. Hearst, "Why phishing works," In *CHI '06: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pp. 581–590, New York, 2006, ACM Press.

[13] M. Wu, R. C. Miller, and S. L. Garfinkel, "Do security toolbars actually prevent phishing attacks?" In *CHI '06: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pp 601–610, New York, 2006, ACM Press.


Dell Battery Return Program - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Address http://www.dellbatteryprogram.com/
DELL™
Internet

Battery Recall
HOME

If you wish to read the text in another language other than English, please select the preferred language from the below list.

العربيه | 简体中文| Dansk | Deutsch | English | Español | Français
한국어 | 日本語| Nederlands | Norsk | Português | Suomeksi | Swedish

Dear Dell Customer,

Dell has identified a potential issue associated with certain batteries sold with Dell Latitude™, Inspiron™, XPS™ and Dell Precision Mobile Workstation™ notebook computers. In cooperation with the U.S. Consumer Product Safety Commission and other regulatory agencies, Dell is voluntarily recalling certain Dell-branded batteries with cells manufactured by Sony and offering free replacements for these batteries. Under rare conditions, it is possible for these batteries to overheat, which could pose a risk of fire.

Potentially affected batteries were sold with the following models of Dell notebook computers or separately as secondary batteries:

- **Latitude: D410, D500, D505, D510, D520, D600, D610, D620, D800, D810**
- **Inspiron: 500M, 510M, 600M, 700M, 710M, 6000, 6400, 8500, 8600, 9100, 9200, 9300, 9400, E1505, E1705**
- **Precision: M20, M60, M70, M90**
- **XPS: XPS, XPS Gen2, XPS M170, XPS M1710**

In addition, these batteries **MAY** have also been provided in response to service calls. The batteries were shipped to customers between April 1, 2004 and July 18, 2006. The words "DELL" and "Made in Japan" or "Made in China" or "Battery cell made in Japan, Assembled in China" are printed on the back of the batteries. If your battery does not reflect one of these markings it is not part of this recall, and you may exit the site.

There is a two (2) step process to identify if your battery is affected:

1. Check if your battery model **MAY** be affected. If your battery is not listed, you are not affected.
2. Check if your specific battery PPID (Dell Part Piece Identification) is affected. This step is necessary to identify if your battery is affected. Only some batteries within each model are affected. If the battery is subject to this recall you will be automatically connected to a replacement order form.

Step 1: Is your battery model affected?

The following battery models, only, **MAY** be subject to recall:

1K055	C5446	F2100	KD494	W5915	Y1333
3K590	C6269	F5132	OR331	X5308	Y4500
5P474	C6270	GD785	M3006	X5329	Y5466
6P922	D2961	H3191	RD857	X5332	
C2603	D5555	J1524	TD349	X5333	
C5339	D6024	JD616	U5867	X5875	
C5340	D6025	JD617	U5882	X5877	

These part numbers are printed on the back of the battery as illustrated below.

Step 2: Is your specific battery affected by this issue?

To determine whether your battery is affected by this issue, you should Click Here.The website will direct you to find and enter an identification number from the back of your battery so as to determine whether the battery is affected by this issue. If the battery is subject to this recall you will be automatically connected to a replacement order form. Dell will also provide a means for you to return the affected battery for proper disposal.

Please note that only the described batteries are subject to this recall and not the notebook computers themselves.

Batteries subject to recall should not be used while awaiting a replacement battery from Dell. You may continue to use your notebook computer using the AC adapter power cord originally provided with your notebook.

Dell apologizes for the inconvenience caused by this issue. Shipment of quality products always has been and continues to be Dell's foremost concern. As always, if you have questions or concerns about this or any other subject, please feel free to contact

Dell Support in your region.

Enter Battery PPID Number

Additional information is available using the following links:
How to Identify Your Recalled Battery

U.S. Order Status

Copyright 1999-2006
Site Terms | Terms and Conditions of Sale | Technical Support Policy | Privacy Policy | About Dell | Contact Us

(a)

Laptop Battery Recall and Replacement Program - Western European (ISO)
File Edit View Tools Message Help
Reply
Reply All
Forward
Print
Delete
Previous
Next
Addresses
DELL™

From: Dell Support
Date: Wednesday, September 13, 2006 11:02 AM
To: John Doe
Subject: Laptop Battery Recall and Replacement Program

Dear Dell Customer,

Dell has identified a potential issue associated with certain batteries sold with Dell Latitude™, Inspiron™, XPS™ and Dell Precision Mobile Workstation™ notebook computers. In cooperation with the U.S. Consumer Product Safety Commission and other regulatory agencies, Dell is voluntarily recalling certain Dell-branded batteries with cells manufactured by Sony and offering free replacements for these batteries. Under rare conditions, it is possible for these batteries to overheat, which could pose a risk of fire.

To find out if your battery is at risk, please click:

http://www.dellbatteryreplacements.com/

Dell apologizes for the inconvenience caused by this issue. Shipment of quality products always has been and continues to be Dell's foremost concern. As always, if you have questions or concerns about this or any other subject, please feel free to contact us at support@dell.com.

Thank you,

Dell Support

Copyright 1999-2006
Technical Support Policy | Privacy Policy | About Dell | Contact Us

(b)

Address http://www.dellbatteryprogram.com/

(c)

To find out if your battery is at risk, please click:

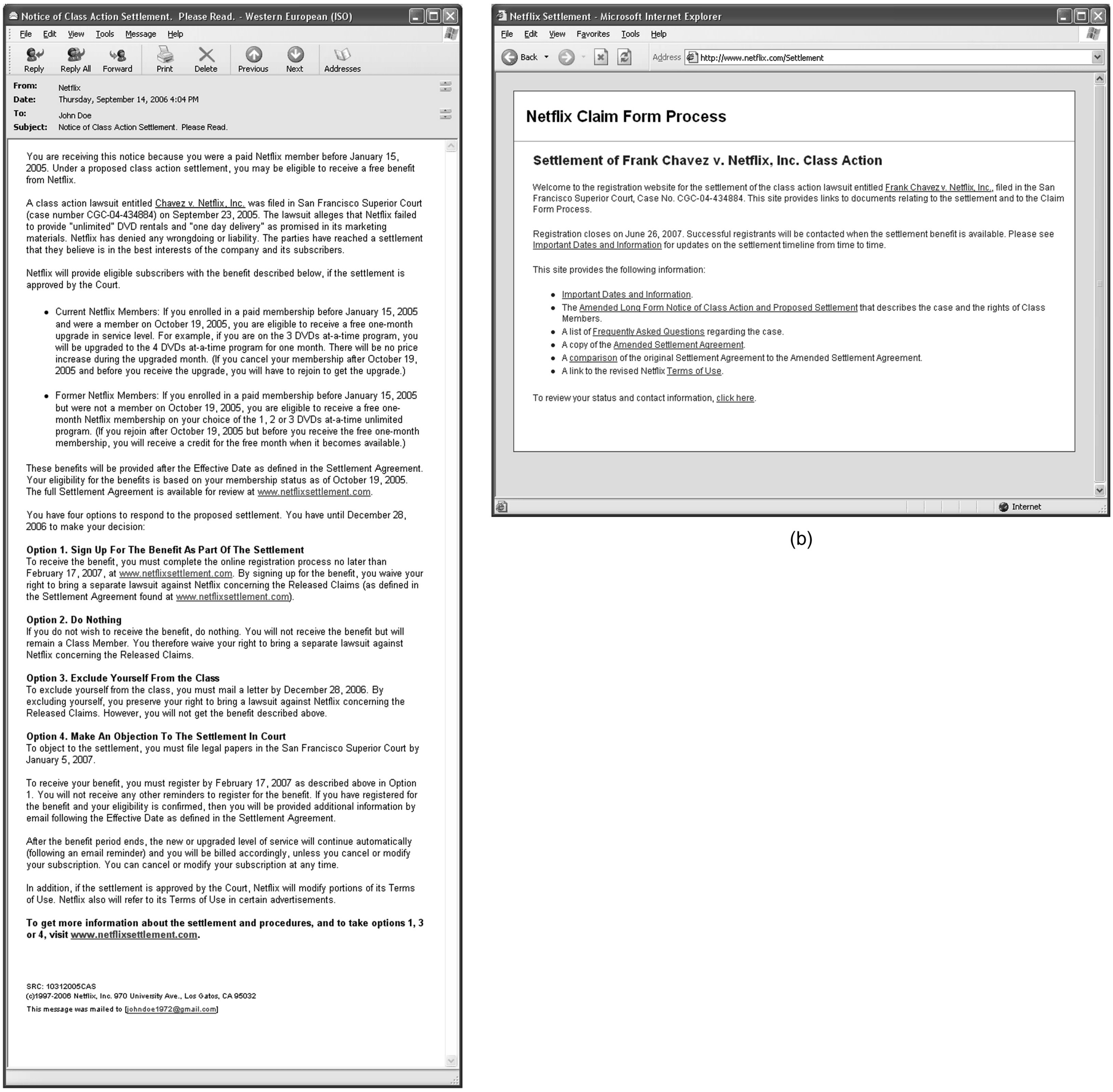
http://www.dellbatteryreplacements.com/

(d)

FIGURE e49.12 (a) The official Dell Battery Return Program Web page. (b) a letter to Dell customer; (c) genuine Web site URL detail; (d) bogus email body detail.

the page content. Though subjects gave a higher average rating to our modified Citibank cardmembers login page, the test showed that the two distributions were not significantly different ($p = 0:133$).

The last test pair was nearly significant ($p = 0:65$) but does not confirm that the two ratings come from different distributions. This pair compared the effects of a plausible parent company domain and subsidiary subdirectory, http://www.ebaygroup.com/paypal/, with the authentic URL that reverses their positions, http://www.paypal.com/ebay/. Although the ebaygroup.com domain is unbound, eBay has registered it. Nevertheless, this test shows a certain flexibility in user acceptance of domain alignment. No PayPal client has seen the PayPal page


Notice of Class Action Settlement. Please Read. - Western European (ISO)
File Edit View Tools Message Help
Reply
Reply All
Forward
Print
Delete
Previous
Next
Addresses

From: Netflix
Date: Thursday, September 14, 2006 4:04 PM
To: John Doe
Subject: Notice of Class Action Settlement. Please Read.

You are receiving this notice because you were a paid Netflix member before January 15, 2005. Under a proposed class action settlement, you may be eligible to receive a free benefit from Netflix.

A class action lawsuit entitled Chavez v. Netflix, Inc. was filed in San Francisco Superior Court (case number CGC-04-434884) on September 23, 2005. The lawsuit alleges that Netflix failed to provide "unlimited" DVD rentals and "one day delivery" as promised in its marketing materials. Netflix has denied any wrongdoing or liability. The parties have reached a settlement that they believe is in the best interests of the company and its subscribers.

Netflix will provide eligible subscribers with the benefit described below, if the settlement is approved by the Court.

- Current Netflix Members: If you enrolled in a paid membership before January 15, 2005 and were a member on October 19, 2005, you are eligible to receive a free one-month upgrade in service level. For example, if you are on the 3 DVDs at-a-time program, you will be upgraded to the 4 DVDs at-a-time program for one month. There will be no price increase during the upgraded month. (If you cancel your membership after October 19, 2005 and before you receive the upgrade, you will have to rejoin to get the upgrade.)

- Former Netflix Members: If you enrolled in a paid membership before January 15, 2005 but were not a member on October 19, 2005, you are eligible to receive a free one-month Netflix membership on your choice of the 1, 2 or 3 DVDs at-a-time unlimited program. (If you rejoin after October 19, 2005 but before you receive the free one-month membership, you will receive a credit for the free month when it becomes available.)

These benefits will be provided after the Effective Date as defined in the Settlement Agreement. Your eligibility for the benefits is based on your membership status as of October 19, 2005. The full Settlement Agreement is available for review at www.netflixsettlement.com.

You have four options to respond to the proposed settlement. You have until December 28, 2006 to make your decision:

Option 1. Sign Up For The Benefit As Part Of The Settlement
To receive the benefit, you must complete the online registration process no later than February 17, 2007, at www.netflixsettlement.com. By signing up for the benefit, you waive your right to bring a separate lawsuit against Netflix concerning the Released Claims (as defined in the Settlement Agreement found at www.netflixsettlement.com).

Option 2. Do Nothing
If you do not wish to receive the benefit, do nothing. You will not receive the benefit but will remain a Class Member. You therefore waive your right to bring a separate lawsuit against Netflix concerning the Released Claims.

Option 3. Exclude Yourself From the Class
To exclude yourself from the class, you must mail a letter by December 28, 2006. By excluding yourself, you preserve your right to bring a lawsuit against Netflix concerning the Released Claims. However, you will not get the benefit described above.

Option 4. Make An Objection To The Settlement In Court
To object to the settlement, you must file legal papers in the San Francisco Superior Court by January 5, 2007.

To receive your benefit, you must register by February 17, 2007 as described above in Option 1. You will not receive any other reminders to register for the benefit. If you have registered for the benefit and your eligibility is confirmed, then you will be provided additional information by email following the Effective Date as defined in the Settlement Agreement.

After the benefit period ends, the new or upgraded level of service will continue automatically (following an email reminder) and you will be billed accordingly, unless you cancel or modify your subscription. You can cancel or modify your subscription at any time.

In addition, if the settlement is approved by the Court, Netflix will modify portions of its Terms of Use. Netflix also will refer to its Terms of Use in certain advertisements.

To get more information about the settlement and procedures, and to take options 1, 3 or 4, visit www.netflixsettlement.com.

SRC: 10312005CAS
(c)1997-2006 Netflix, Inc. 970 University Ave., Los Gatos, CA 95032
This message was mailed to [johndoe1972@gmail.com]

(a)

Netflix Settlement - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Address
Internet

http://www.netflix.com/Settlement

Netflix Claim Form Process

Settlement of Frank Chavez v. Netflix, Inc. Class Action

Welcome to the registration website for the settlement of the class action lawsuit entitled Frank Chavez v. Netflix, Inc., filed in the San Francisco Superior Court, Case No. CGC-04-434884. This site provides links to documents relating to the settlement and to the Claim Form Process.

Registration closes on June 26, 2007. Successful registrants will be contacted when the settlement benefit is available. Please see Important Dates and Information for updates on the settlement timeline from time to time.

This site provides the following information:

- Important Dates and Information.
- The Amended Long Form Notice of Class Action and Proposed Settlement that describes the case and the rights of Class Members.
- A list of Frequently Asked Questions regarding the case.
- A copy of the Amended Settlement Agreement.
- A comparison of the original Settlement Agreement to the Amended Settlement Agreement.
- A link to the revised Netflix Terms of Use.

To review your status and contact information, click here.

(b)

FIGURE e49.13 (a) Low-profile class-action suit. (b) a lengthy notice that describes a class-action lawsuit against Netflix, a settlement to the lawsuit, and options for claiming benefits.

displayed under the http://www.ebaygroup.com/paypal/ address, yet their authenticity ratings are not significantly different. This result furthers our conviction that semantic alignment between content and URL is a principal factor in authenticity evaluations.

The last two Web stimuli sets are not twins; they are the Dell battery replacement page and the Netflix settlement page. Both pages are authentic, although the content of the Netflix page was altered to appear relevant at the time of testing. They received polar opposite ratings. The Dell battery page was statistically indistinguishable from the highest-rated page (the authentic PayPal site), and the Netflix page rated dead last—significantly lower than the second lowest rating ($p = 1{:}20\ 10^{-7}$). As mentioned before, the Dell battery program stimuli benefit from a high visibility news story. It's noteworthy that the URL in the Web page (authentic) is different from the URL in the email (phishing), which subjects saw first. Subjects did not penalize the Web page for this inconsistency. Subjects may have had difficulty constructing a phishing

TABLE e49.1 The Other Third Party Attack.

Stimulus Description	Mean	Diff.	χ^2	*p*
Chase card payment statement (legit)—plain layout	3.40	0.36	11.89	0.018
Chase card payment statement (legit)—fancy layout	3.76			
Chase phish-fancy layout	3.19	0.02	6.31	0.177
Chase phish-plain layout	3.18			
AT & T Universal Card statement without legal notices	3.05	0.62	30.18	0
AT & T Universal Card statement with legal notices	3.66			
PayPal policy change + VeriSign	3.19	0.11	5.75	0.219
PayPal policy change − no VeriSign	3.30			
Citibank phish − no VeriSign	2.40	0.29	9.62	0.047
Citibank phish + VeriSign	2.69			
AT & T Universal card login				
https://www.accountonline.com/View?docId = Index & siteId = AC & langId = EN	2.76	0.49	15.46	0.004
http://www.attuniversalcard.com	3.25			
Citbank (phish); URL = http://www.citicardmembers.com/	3.11	0.32	7.06	0.133
Copy of original site;	3.43			
Logos modified to better match domain				
PayPal Web site displaying eBay logo:				
URL = http://www.ebaygroup.com/paypal/	3.35	0.35	8.83	0.065
URL = http://www.paypal.com/ebay/	3.70			
Indiana University Credit Union homepage:				
Deemphasizes security language; no mention of “ attacks “	3.69	0.32	11.45	0.022
Phishing attack banner + strong fraud warnings	3.37			
Wells Fargo phishing page:				
Reproduces original content;	3.17	0.31	10.83	0.029
URL = http://www-wellsfargo.com/				
Adds VeriSign endorsement; uses SSL;	3.48			
URL = https://www-wellsfargo.com/				
Netflix class-action settlement email (authentic)	2.72			
Netflix class-action settlement homepage (authentic)	2.55			
Dell battery replacement email (phishing)	3.61			
Dell battery replacement Web page (authentic)	3.54			

Note: The first section of the table reports on the differences between email messages; the next section reports on the Web pages; and the last section gives the average rating for the third-party attacks.

scenario based on the informational nature of the page; there is no request for personal information.

Similarly, the Netflix settlement page does not make any overtures for personal information. Even more surprising is that the URL http://www.netflix.com/settlement/ aligns well with the content. Subjects may have dismissed the page based on mistrust of the email stimulus, which they viewed prior to (several screenshots before) the Web stimulus. The Netflix page is notable for its brevity and unsophisticated layout. It is the only page

An Agenda for Action for Social Engineering Tactics

Our results forecast the following social engineering tactics: (Check All Tasks Completed):

_____**1.** Construct messages with weak narratives (bordering on innocuous) but use strong design elements (graphics, small-print footer, endorsement logos) and identifying information to improve authenticity impressions.

_____**2.** Use softer bait. Messages that do not encapsulate an imminent request for information, such as the Dell battery bait, rated highly in the test.

_____**3.** Use plausibly unfamiliar administration pages; for example, the Dell Battery Return Program Web site provides a service that is not typically seen, such as a login page (so visitor expectations are less concrete).

_____**4.** Leverage high-profile news to produce messages with credible and strong narratives. Personalization will be less important in these cases.

_____**5.** Align domain names with page content. Although subjects were turned off by semantic mismatches between domain names and content, they were insensitive to malformed links (http://www-wellsfargo.com).

without graphics or logos of any kind. There are no apparent links back to the primary Netflix page. With the exception of the blue underlined hyperlinks and gray margins, the page is black and white. We take from this rating that utilizing minimalist design is a poor strategy for unsolicited communications, even for important and serious matters such as law.

3. IMPLICATIONS FOR CRIMEWARE

The experiment focused on design features and their effect on people's ability to distinguish authentic email and Web sites from malicious forgeries. Although presented in the context of phishing, we do not measure how often subjects disclose passwords or other sensitive data; rather, we identify design principles that convey authenticity. Just as phishing bait promises resolution upon revealing information, social crimeware bait may promise resolution contingent upon installing browser extensions or accepting self-signed Java applets. Presenting a convincing false identity to the victim is essential in both contexts (see checklist, "An Agenda For Action For Social Engineering Tactics").

With respect to the final point, the "rock-phish" gang has proven that effective domain alignment can be achieved through deceptive subdomains,[14] the control of which is delegated to the domain owner rather than the registrar. The following URL, from a social engineering attack in the wild, illustrates this tactic:

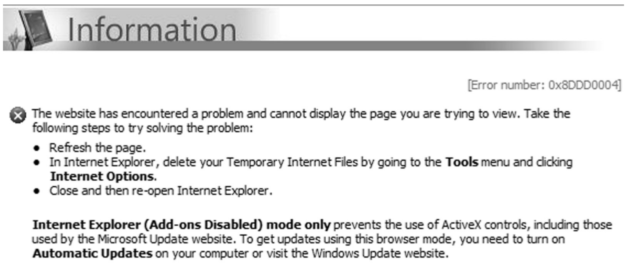
www.paypal.com.cgi.bin.account.webscr.cmd.login.
run.php.draciimasi.info/webscr.php?cmd = Login

The registered domain is draciimasi.info, but the owners have prepended it with a deep subdomain. Since subjects accepted the substitution of a dash for a dot in www-wellsfargo.com, they could easily accept a dot for a slash, as above. Moreover, the preponderance of subdirectory names such as cgi, bin, webscr, and the like further clouds the issue for the technically uninformed. This tactic may be particularly effective for download pages because they tend to be buried several directories deep; login pages, on the other hand, are frequently in the root of a domain.

Example: Vulnerability of Web-Based Update Mechanisms

Legitimate Web sites often make their services contingent upon changing settings, installing extensions, or accepting certificates. One important example is Microsoft's Windows Update Web site. It scans the client for installation detail through ActiveX extensions. When accessing the Web site through a professionally managed client at Indiana University, an update is not possible because the administrators have disabled the service. However, the Web site (see Figure e49.14) suggests workarounds involving settings changes.

None of these suggestions will enable remote update for this professionally managed computer, but subtle



Information

[Error number: 0x8DDD0004]

The website has encountered a problem and cannot display the page you are trying to view. Take the following steps to try solving the problem:

- Refresh the page.
- In Internet Explorer, delete your Temporary Internet Files by going to the **Tools** menu and clicking **Internet Options**.
- Close and then re-open Internet Explorer.

Internet Explorer (Add-ons Disabled) mode only prevents the use of ActiveX controls, including those used by the Microsoft Update website. To get updates using this browser mode, you need to turn on **Automatic Updates** on your computer or visit the Windows Update website.

FIGURE e49.14 Suggested workarounds involving settings changes.

[14] T. Moore and R. Clayton, "An empirical analysis of the current state of phishing attack and defense," The 2007 Workshop on the Economics of Information Security (WEIS 2007), 7–8 June 2007.

changes to the instructions could cause unsophisticated users to disengage important access controls. For example, the user could have been instructed to enter Addons Enabled mode. Subsequent installation of malicious addons will lead to a compromise. As long as the host's identity has been convincingly spoofed, users will be vulnerable to these kinds of attacks.

Example: The Unsubscribe Spam Attack

This attack leverages the first two tactics we discussed: weak narrative combined with strong design elements and softer bait. Some of the most highly rated email messages avoided hyperlinks in the main message text. The Chase account payment was completely devoid of hyperlinks and instead directed receivers to type www.chase.com into their address bar. Similarly, the PayPal message had no hyperlinks in its body, but it included a hyperlink in the footer to change preferences. The highly rated AT&T Universal card promotion also contains links in its small-print footer.

The attacker will send out promotional email that appears to come from the spoofed institution. The promotion would employ a weak narrative to shift user attention to a plethora of design features (graphical header, footer, small print, personalization, genuine but unlinked URLs in the body, and so on). The body will generate the perception of authenticity by referring the receivers to the phone number on back of her credit card or by requiring users to manually type in the promotional URL. Among the design features is a small-print footer with an unsubscribe hyperlink. This link will take users to a Web page that spreads crimeware simply by loading malicious JavaScript code, like a "drive-by pharming attack."

The bait message gets users to click on the link indirectly: annoyance with the volume of unsolicited messages. No suspicion is aroused through directions to change settings; the malware spreads on load.

The Strong Narrative Attack

The strong narrative attack engages the receiver with a plausible story, often bundling actions to well-known news stories. The Chase phishing message that promotes ePIN to incoming Bank One customers is such an example; it leverages in the news of the Bank One acquisition. The Dell battery program stimuli gain most of their credibility from the story's media coverage. The message maintains this credibility by deferring the request for personal information; standard attacks request an "account login" or "settings update" in the message body. This battery exchange program could have been turned into a "patch-now" attack by claiming that a firmware or operating system fix would prevent overheating.

Though scams that exploit strong narratives and current events are not new (many fraud cases capitalized on the September 11, 2001, and Hurricane Katrina tragedies[15,16]), our research suggests that they are less influenced by design features. This finding is supported by the persistence of the Nigerian code 419 advance fee scams.[17] One widespread form of this attack entices victims with a story of the death of a foreign dignitary and the need to move large amounts of money (allegedly to protect it from corrupt enemies); they offer the victim a cut for moving the money. After drawing the victim into this illusion, the scammers request advance fees to enable the transfer of money. These messages break many design rules that promote trust: They use poor spelling and grammar, email messages are often plaintext, return addresses are essentially anonymous using free email accounts. Yet these scams still account for large amounts of Internet fraud, exceeding $3 billion in losses according to some estimates.[18]

SUMMARY

This study tested the impact of several document features on user authenticity perceptions for both email messages and Web pages. The influence of these features was context dependent in email messages. We were surprised that this context was shaped more by a message's narrative strength, rather than its underlying authenticity. Third-party endorsements and glossy graphics proved to be effective authenticity stimulators when message content was short and unsurprising. The same document features failed to influence authenticity judgments in a significant way when applied to more involving messages. Most surprising was the huge increase in trust caused by a small-print footer in a message that already exhibited strong personalization with its greeting and presentation of a four-digit account number suffix.

The data suggest a link between narrative strength and susceptibility to trust-improving document features, but the experiment was not designed to test this hypothesis. Future work should characterize more precisely what kind

[15] Fraud Section, Criminal Division, U.S. Department of Justice. Special report on possible fraud schemes, www.usdoj.gov/criminal/fraud/WTCPent-SpecRpt.htm, 27 September 2001, retrieved December 2006.

[16] B. Krebs, "Katrina phishing scams begin," WashingtonPost.com: Security Fix, 31 August 2005.

[17] M. Zuckofi, "The perfect mark: How Massachusetts psychotherapist fell for a Nigerian e-mail scam," *The New Yorker*, 15 May 2006, www.newyorker.com/fact/content/articles/060515fa_fact.

[18] Ultrascan Advanced Global Investigations, "Advance fee fraud in 37 nations," www.ultrascan.nl/html/aff_37_countries.html, 25 March 2006, retrieved December 2006.

of messages can benefit from these features and what kind of messages are resistant to their sway.

Since spoofed Web page content need not differ from the authentic pages, we focused three Web page tests on the effects of semantic alignment between address bar URLs and page content. The first showed a clear statistical preference for a simulated Web page whose domain name matched its content rather than the genuine page whose domain was only weakly aligned with the same content. The second test, which created better alignment with a bogus domain name by altering company logos, failed to register a statistically significant change in authenticity ratings. The third test compared an authentic page (and URL) with an authentic version of the same page content paired with a well-aligned but bogus URL; the results which favored the genuine URL were just shy of statistical significance. In conclusion, we find that URL can change authenticity ratings.

This experiment also verified that it is possible to overuse well-intended notices about security and fraud. We observed a statistically significant negative effect of genuine, but heavy-handed, fraud warnings. Another test showed a statistically significant improvement in authenticity perception when using SSL and a third-party endorsement logo on a fraudulent Web page showing a suspiciously formed, but semantically well-aligned, domain name.

The experiment simulated two sequences (one email and one Web page) that appeared to be third parties charged with handling embarrassing incidents for their corporate clients. Though separated by many variables, one turned out to be among the most trusted stimuli in the test, whereas the other rank among the lowest. The poorly ranked one, though authentic, broke all the rules: poor publicity, long and rambling message, use of third-party domain names, and no graphics. The highly ranked one (whose bogus email message was concocted by the authors) benefited from a widely publicized recall message. The story overrode the message's poor personalization, illegitimate URL, and relatively simple layout.

These factors offer a glimpse into what kinds of social engineering tactics may be deployed in the future. We describe an unsubscribed attack which contains an innocuous message, many authenticity stimulating document features, and an unsubscribe link that leads to a noninteractively infectious Web site. Our tests with third-party administration suggest that organizations in the process of correcting an embarrassing incident are highly vulnerable to social engineering attacks. Finally, our findings suggest some common pitfalls for legitimate Internet communications to avoid: overuse of fraud warnings, utilization of poorly aligned domain names, failure to use HTTPS for rendering login pages, and long or rambling email messages.

Finally, let's move on to the real interactive part of this Chapter: review questions/exercises, hands-on projects, case projects and optional team case project. The answers and/or solutions by chapter can be found in the Online Instructor's Solutions Manual.

CHAPTER REVIEW QUESTIONS/EXERCISES

True/False

1. True or False? Identity theft is commonly defined as unwanted appropriation of access credentials that allows creation and access of accounts and that allows the aggressor to pose as the victim.
2. True or False? Phishing is a form of Internet fraud that spoofs emails and Web pages to trick people into disclosing sensitive information.
3. True or False? Web sites, particularly the login and information collection pages associated with phishing scams, do present a story the way email messages do.
4. True or False? One way phishers align page content with URLs is by choosing an apt domain name; the other way is to change the page content.
5. True or False? Legitimate Web sites often make their services contingent upon changing settings, installing extensions, or accepting certificates.

Multiple Choice

1. An attacker will send out ___________ that appears to come from the spoofed institution.
   A. Privacy-enhancing technology
   B. Location technology
   C. Promotional email
   D. Executable policies
   E. Data controller
2. What message gets users to click on the link indirectly: annoyance with the volume of unsolicited messages?
   A. Policy enforcement
   B. Location technology
   C. Valid
   D. Environmental data
   E. Bait
3. What attack engages the receiver with a plausible story, often bundling actions to well-known news stories?
   A. Data minimization
   B. XACML
   C. Privacy risks
   D. Strong narrative
   E. Security

4. What is a type of identity theft that is perpetrated on the Internet and that typically relies on social engineering to obtain the access credentials of the victim?
   - **A.** Privacy metrics
   - **B.** Greedy strategy
   - **C.** Sensitive information
   - **D.** Phishing
   - **E.** Taps
5. What is often defined as economically motivated malware?
   - **A.** Irrelevant
   - **B.** Sensor nodes
   - **C.** Crimeware
   - **D.** Disclose-to
   - **E.** Server policy

EXERCISE

Problem

You should never respond or reply to an e-mail, phone call, or text message that?

Hands-on Projects

Project

How can one enhance the security of their transactions and experiences on the Internet and better control any related risks?

Case Projects

Problem

Occurrences of identity theft continue to increase. Please explain identity theft, and how you might avoid becoming a victim?

Optional Team Case Project

Problem

What should one do if he or she have become a victim of identity theft?