USA TODAY Education

GREAT AMERICAN FINANCIAL RESOURCES

Special Reprint Edition
As seen in USA TODAY,
November 28, 2007

Typos can lead to imposter sites

By Byron Acohido

SEATTLE — Sloppy keyboarding can add to your confusion as you search online for your credit data.

At USA TODAY's request, anti-virus firm Symantec checked two high-traffic websites — FreeCreditScore.com, operated by Experian, and TrueCredit.com, operated by TransUnion — and found hundreds of "typo squatters" misdirecting consumers to imposter Web pages.

Typo squatters set up Web pages with Internet addresses that are slightly different from the location of the official site. Their aim: to capture visits from Web users who mistype the official address.

Oliver Friedrichs, Symantec's director of emerging technologies, found 236 variations of FreeCreditReport.com and 114 variations of TrueCredit.com.

Most of the imposter sites routed visitors to still other websites selling credit-related services, thereby earning an advertising kickback, says Friedrichs.

A couple of examples: freecreditrepotrt.com, registered to Caribbean Online International Ltd., and trudecredit.com, registered to Wan-Fu China Ltd. A visitor to these pages sees a bare bones listing of links to other commercial sites selling credit services.

Imposter sites typically lack privacy policies and contact information, according to a 2005 study by the World Privacy Forum.

That 2005 study found typo squatters operating 233 websites with addresses similar to AnnualCreditReport.com, the website that distributes free credit reports as mandated by federal law. Researchers found one imposter site collecting Social Security numbers to share with other companies. The site was taken offline in June 2005.

Consumers should expect the worst from imposter sites. "Typo squatters act in bad faith," says Friedrichs. "In most cases, these sites are registered for the purposes of advertising, but they can also host malicious activities."

"Typos can lead to imposter sites": Protecting yourself against online financial scams

Objectives

- Read the article "Typos can lead to imposter sites."
- Define "typo squatter."
- List the potential dangers of imposter websites.
- Identify real and fake Web addresses by playing the online game, Anti-Phishing Phil.
- State the steps that victims of a phishing attack should take.

Preparation

Each student will need:

- A copy of the article "Typos can lead to imposter sites."
- Internet access to play Anti-Phishing Phil. If Internet access is not available, contact Lorrie Cranor of Carnegie Mellon University at 412-268-7534 for a free downloadable, non-commercial version.
- A copy of the takeaway "How can I identify a phishing website."

1. Read the article and answer discussion questions. (20 minutes)

- What is the main point of this article?
- What is a "typo squatter"?
- What are some indications that a website may not be trustworthy?
- What is a potential danger of these imposter websites?
- Have you come across one of these websites?
- How did you know it was a fake?
- What did you do?
- What should you do?

2. Play Anti-Phishing Phil and spot the scammers. (20 minutes)

Anti-Phishing Phil is an interactive game that teaches users how to identify phishing URLs (Web addresses), where to look for clues in Web browsers and how to use search engines to find legitimate sites. Anti-Phishing Phil is an entertaining way to learn about phishing attacks and how to avoid them.

Directions: There are four rounds to the game. Each round has 10 worms. As you put the mouse on each worm, a URL will appear. If the URL is a legitimate site, Phil should eat it. If, however, the URL is a fake and Phil eats it, he is hooked by the bait and loses 10 seconds. If Phil is unsure, you can hit the T key and get his dad's advice. In-between rounds, Phil's dad teaches him a little bit more about identifying fake websites and spoofs. Be aware of the other predators like eels and sharks and keep an eye on the time. The game gives a brief introduction including the keys needed to play. Keep track of how many you get right the first time. If your teacher chooses, winners may receive snack packs of Goldfish crackers or Swedish Fish gummy candies. The game Web address is http://cups.cs.cmu.edu/antiphishing_phil/new/index.html.

3. Debrief and apply. (10 minutes)

- How well did you do with Anti-Phishing Phil?
- What did you discover about identifying fake websites?
- How can you verify the validity of real websites?
- What can you do if you're not sure?
- What steps should you take if you're a target of a phishing attack?

How can I identify a phishing website?

- Avoid being a victim: Recognize common tactics used by Internet imposters.
- Be wary of e-mails from people you don't know or trust. Delete any e-mails you think are suspicious.
- Never click on a link or an attachment in an e-mail from a source you don't know or trust. Phishing e-mails contain links to websites that may look legitimate and ask for personal and financial information. However, if you use your mouse and hover over the link, you can see the actual Web address it will link to. If it doesn't have an "https:" address, it's not a secure site — one clue that the site may not be real. If you think the e-mail link might be authentic, type the Web address you're supposed to go to into your Web browser and go from there.
- Make sure you've typed the Web address (URL) in correctly. Phishers often use slightly misspelled company names in their URL such as www.paypa1.com (a "1" instead of the "l" in Paypal).
- Never provide your personal or security details, including customer IDs or passwords, in response to any e-mail. Reputable companies will never request this information from you via e-mail. Be especially wary of pop-ups. Some phishing sites will direct you to a legitimate website but then request personal information in the pop-up.
- Always scan any new programs or files for viruses before you open, install or use them. Your anti-virus software may do this for you automatically.
- Many phishing e-mails' websites have poor grammar and spelling (although sometimes they can be grammatically perfect).
- Be wary of urgent appeals for help or personal details (like credit card or account numbers, PINs or passwords). Some phishing e-mails will request your correct address, name of your bank and home phone number. Sometimes just this information alone makes it easy for scammers to steal your identity.