

Larry's newsLETTER

As disasters spread, so do online scammers

The outpouring of generosity from people all over the world following the earthquake in Japan has been accompanied by a profusion of donation scams.

These scams no longer prey on the simply gullible but have moved to less obvious ruses such as malicious websites that use **clickjacking** and **drive-by** attacks.

Natural disasters bring out extremes of human behavior. Workers at the devastated Japanese nuclear power plants place themselves in harm's way trying to protect other people from explosions and radiation poisoning. Military and social services staffers work days without sleep under horrifying conditions.

And in response, strangers around the world ask how they can help, what they can do, what they can send. Unfortunately, predators also respond, seeking to exploit the suffering and generosity of others for personal gain.

Online donation scams are not new, but they became really evident in 2005 in the aftermath of Hurricane Katrina. Most of those scams were e-mail-based phishing, also known as 419 scams. The least sophisticated claimed to be from victims; they explained complicated and peculiar circumstances leading them to write e-mails asking individuals for money. More advanced phishing scams imitated the look and feel of reputable charities' Web presences.

Thanks to the increasing efficiency of spam filters, e-mails such as these reach fewer users today - and most Web users have learned to recognize and discard them quickly.

Since 2005, online scams have grown in sophistication. So it should be no surprise that, in the wake of Japan's crisis, donation scams are harder to spot. Clickjacking and drive-by threats don't depend on our charitable impulses — they target our interest in the unfolding events, using such common sources as news photographs, links to YouTube videos, and information updates.

Since March 11, 2011, scores of domain names have been registered — names containing terms such as Japan help, tsunami, or nuclear disaster, according to a Forbes [report](#).

Often, these URLs are similar to the Web addresses of popular sites or are based on common misspellings. These malicious sites are also heavily seeded with now-familiar search terms (Japan, tsunami, nuclear disaster, radiation, Japan help, and so on) to draw the clicks of (or clickjack) people searching for information. This practice is known as **search engine optimization poisoning**.

A TrendMicro [blog](#) shows a search return list that reportedly includes fake sites.



Techie Term:

404 Error

A 404 error is a common website error message that indicates a webpage cannot be found. It may be produced when a user clicks an outdated (or "broken") link or when a URL is typed incorrectly in a Web browser's address field. Some websites display custom 404 error pages, which may look similar to other pages on the site. Other websites simply display the Web server's default error message text, which typically begins with "Not Found." Regardless of the appearance, a 404 error means the server is up and running, but the webpage or path to the webpage is not valid.

So why call it a "404 error" instead of simply a "Missing Webpage Error?" The reason is that 404 is an error code produced by the Web server when it cannot find a webpage. This error code is recognized by search engines, which helps prevent search engine crawlers from indexing bad URLs. 404 errors can also be read by Web scripts and website monitoring tools, which can help webmasters locate and fix broken links.

Larry's newsLETTER

Sometimes the scams are relatively innocuous; scammers register these bogus Web addresses as a way to earn money through advertising or delivering traffic to online survey sites. But others are far more dangerous. Clicking malicious drive-by sites, for example, can easily result in an infected PC.

Search-engine companies watch for these sites and eliminate the dangerous ones as quickly as possible. But so many have appeared in the aftermath of Japan's disaster that even Google is having difficulty keeping up with them, [reports](#) Bojan Zdrnja at Internet Storm Center.

PC users can also be directed to drive-by sites through links circulated on Twitter, Facebook, and other social-networking sites as well as in discussion forums. Wall posts, IMs, and messages represent themselves as containing links to newly uncovered disaster videos that might be tsunami simulations, doctored images, and worse.

"Facebook users are being tricked into clicking on links which claim to be raw CNN footage of the Japanese tsunami by cold-hearted scammers — as part of a plot to earn money by driving Web traffic to take online surveys. The videos, which in the examples seen by Sophos exist on a website called spinavideo, purport to be footage of the horrifying tsunami which hit parts of Japan on Friday."

Clicking the link takes users to a spoof website that looks like YouTube. Users are tricked into agreeing to 'Like' the page on Facebook, which spreads the scam even further on Facebook.

But misdirection to online surveys and **likejacking**, as Cluley describes above, can be the least of a deceived user's problems. A user who activates a clickjacking link is taken to a drive-by website that might (or might not) look legitimate but that automatically downloads malware onto the user's machines. The most frequently downloaded type of malware is rogue security software, often also called rogue antivirus software (or rogue AV).

Rogue security software masquerades as legitimate security software. Sometimes it even imitates legitimate security software interfaces, such as Microsoft Update. After it's installed on your machine, antivirus malware might simply pretend to detect viruses and then entice you into paying for a **subscription** to have your machine **cleaned**.

Or it might install more malicious software — keyloggers, password recorders, or rootkits — that can go undetected while stealing your data. This software might lie dormant until it detects a specific event, such as when you enter a bank account number. Then it comes to life and starts collecting your keystrokes: recording your passwords, social security number, date of birth, and other personal data.

The scammers resell your credit card numbers or passwords to other criminals.



This Months Quote:

Computing is not about computers any more. It is about living.

~Nicholas Negroponte



Larry's newsLETTER



Larry The Computer Guy

5307 Carroll Lake Rd

Commerce MI 48382

248-360-8967

Then they change their company name, change the credit agency they're using to bill you for your "malware subscription," and vanish before they can be identified. Rogue security software costs the banking industry billions of dollars a year, a cost borne by consumers.

Gleened from Windows Secrets 3/24/11 Edition

How to keep yourself safe in disastrous times

Here are tips to help you protect yourself from donation fraud:

- Make informed choices about where to donate. Before turning over the personal information needed to process your donation, visit an online watchdog site such as charitywatch.org to evaluate the receiving organization's legitimacy.
- Don't click links in online forums, e-mails, or IMs that say they are from charity organizations — even well-known ones such as the Red Cross or Red Crescent, Mercy Corps, World Vision, or others. These e-mails could easily be spoofs that will direct you to a website that looks like the real thing but steals your data.
- Do not respond to unsolicited requests for donations, particularly from people who claim to be victims. "Symantec has observed a classic 419 message targeting the Japanese disaster," said researcher Samir Patil in a post to the company's security blog. "The message is a bogus 'next of kin' story that purports to settle millions of dollars owing to an earthquake and tsunami victim."
- To get to the website of a charitable organization you want to support, type its web address into your browser's address bar yourself — don't rely on links, however professionally designed they may look, to take you there.
- When you are on a charitable site, take a moment to check the spelling of the organization's website in the address bar. Scammers often use common typos or misspellings to create URLs that fool an unwary eye.

Make sure the page where you enter your credit card or other personal information is encrypted. The beginning of the address should read **https://** instead of **http://**.

- Make sure any site that you donate through has a written privacy policy.
 - Get your news about events in Japan from reputable news sites.
- If you believe you have been a victim of a charity-related scam, contact the National Center for Disaster Fraud by telephone at (866) 720-5721, by fax at (225) 334-4707, or by e-mail at disaster@leo.gov.

You can also keep an eye on samples of fraudulent e-mails and messages by watching the forums at ScamWarners, a reputable Internet Fraud Center that will also examine and evaluate material you submit and post samples to help other people avoid being scammed.

Gleened from Windows Secrets 3/24/11 Edition

If your computer speaks English, it was probably made in Japan.

Alan Perlis



Larry's newsLETTER



Larry The Computer Guy

5307 Carroll Lake Rd

Commerce MI 48382

248-360-8967



Last years Tax return; What am I going to do with this Years?



Computer Quotes

Hardware: where the people in your company's software section will tell you the problem is.

Software: where the people in your company's hardware section will tell you the problem is.

Larry The Computer Guy: Where we don't point fingers we just fix it.

~Dave Barry, Claw Your Way to the Top; LTCG

If you have any trouble sounding condescending, find a Dell or HP tech support person to show you how it's done.

~Author Unknown

I just wish my mouth had a backspace key.

~Author Unknown

If it draws blood, it's hardware.

~Author Unknown

Larry's newsLETTER



Larry The Computer Guy

5307 Carroll Lake Rd

Commerce MI 48382

248-360-8967



Quality Education for your Children

Interested in a Christ-centered education?

St. Matthew Lutheran School registering for the 2011/2012 school year.

- Located in Walled Lake
- Grades - Preschool through Grade 8
- Quality academic and spiritual education to students for over 50 years
- We are an accredited school with highly qualified and state trained teachers.
- We focus on educating the whole child, but our top priority is cultivating and nurturing your child's relationship with Jesus Christ.



To learn more or set up an appointment Call 248-624-7677

Larry's newsLETTER



Larry The Computer Guy
5307 Carroll Lake Rd
Commerce MI 48382
248-360-8967

Compare **our** check Prices!

Voucher	250	500	1000	2000	5000
Peachtree	\$81.95	\$106.95	\$147.95	\$239.95	\$599.87
Nebbs	\$82.50	\$113.50	\$154.50	\$259.95	\$649.87
McBee	\$82.50	\$113.50	\$154.50	\$259.95	\$649.87
Deluxe	\$82.50	\$113.50	\$154.50	\$259.50	\$649.87
Intuit	\$79.99	\$109.99	\$149.99	\$239.99	\$599.87
Nelco	\$103.45	\$137.85	\$188.00	\$343.40	\$637.00
Greatland	\$103.45	\$137.85	\$188.00	\$343.40	\$637.00
LTCG	\$63.75	\$79.90	\$101.15	\$154.70	\$280.50

Larry The Computer Guy

248-360-8967

We have partnered with several different companies to provide a wider range of services.

We now offer low cost printer ink and toner.
Check our Prices delivered to your door for 30% less than office supply stores.

Are you tired of all that spam in your mailbox?

We have partnered with Spam Bully and offer a 10% discount on the product. Call us for more information or to sign up.

Tired of remembering all those passwords for all your different websites?

We have also partnered with Roboform and offer a 10% discount on the product. Call us for more information or to sign up.

Larry's newsLETTER



Larry The Computer Guy

5307 Carroll Lake Rd

Commerce MI 48382

248-360-8967



[Photos: Germany's upside-down house](#)

Website Hosting and Design

We offer full website hosting including email and design.

Call us for a free quote.

248-360-8967

These documents are provided for informational purposes only. The information contained in this document represents the current view of VHC Enterprises DBA Larry The Computer Guy on the issues discussed as of the date of publication. Because VHC Enterprises must respond to changes in market conditions, it should not be interpreted to be a commitment on the part of VHC Enterprises and cannot guarantee the accuracy of any information presented after the date of publication.

INFORMATION PROVIDED IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND FREEDOM FROM INFRINGEMENT.

This newsletter and website may contain links to other websites with whom we may or may not have a business relationship. VHC Enterprises DBA Larry The Computer Guy does not review or screen these sites, and we are not responsible or liable for their privacy or data security practices, or the content of these sites. Additionally, if you register with any of these sites, any information that you provide in the process of registration, such as your email address, credit card number or other personally identifiable information, will be transferred to these sites. For these reasons, you should be careful to review any privacy and data security policies posted on any of these sites before providing information to them.

The user assumes the entire risk as to the accuracy and the use of this document. This document may be copied and distributed subject to the following conditions: 1) All text must be copied without modification and all pages must be included; 2) All copies must contain VHC Enterprises' copyright notice and any other notices provided therein; and 3) This document may not be distributed for profit. All trademarks acknowledged. Copyright VHC Enterprises, Inc. 1991-2008.

To Subscribe or unsubscribe go to www.larrycomputerguy.com and click on the mailing list link or cut and past the following link into your browser:

<http://www.larrycomputerguy.com/subscribe.htm>