

Log In

Like

538k

Member Center

Alerts & Newsletters

Jobs

Cars

Real Estate

Rentals

Weekly Circulars

Local Directory

Place Ad

# Los Angeles Times | BUSINESS



LOCAL U.S. WORLD BUSINESS SPORTS ENTERTAINMENT HEALTH LIVING TRAVEL OPINION SHOP

MONEY & CO. TECHNOLOGY HIGHWAY 1 COMPANY TOWN PERSONAL FINANCE JOBS REAL ESTATE CARS BUSINESS PLUS

TRENDING NOW VENICE BOARDWALK | ALEX RODRIGUEZ | 'WHITEY' BULGER | TEACH FOR AMERICA | BART STRIKE

Search

Cast us in your next production. [SEE OPTIONS](#)

## BREAKING NEWS

At least 12 players suspended by Major League Baseball [Sign up for alerts >>](#)

## Email 'phishing' attacks by hackers growing in number, intensity

Fake emails get harder to distinguish from real ones as hackers use 'phishing' attacks to access company and government data.

Comments 5 Email Share 212 [Tweet](#) 101 [Like](#) 111 [7](#)

Connect

Recommended on Facebook [Like](#) 538k

- My melanoma, my message**  
1,091 people recommend this.
- Federal judge keeps blocking part of Wisconsin abortion law**  
4,890 people recommend this.
- Venice boardwalk crash: Man, 38,**  
suspected as suspicion of murder

advertisement

Technology reporters Paresh Dave and Andrea Chang discuss the growing sophistication of phishing scams and how they continue to flourish.

By Paresh Dave  
July 25, 2013 | 6:09 p.m.

At least 2 million people received the email May 16 notifying them that an order they had just made on "Walmart's" website was being processed, though none of them had done any such thing.

Still, thousands of people clicked on the link in the email, taking many of them to a harmless Google search results page for "Walmart." Others weren't so fortunate. The link led to the invisible download of malware that covertly infected their personal computers, turning them into remotely controlled robots for hackers, according to email security firm Proofpoint Inc.

These sorts of "phishing" attacks are not only becoming more common but also are getting more lethal, with fake emails becoming harder to distinguish from real ones.



Facebook revenue jumps 53% with

In the fake-Wal-Mart attack, people missed clear warning signs — such as the company name being misspelled and the sender's address being very long and strange. But in another case a month later, an email claiming to be from American Airlines carried no visible hints that it was illegitimate.

The sophisticated attacks are targeting the likes of attorneys,

**KNOCK \$1,000 OFF CLOSING COSTS**  
Plus, Get a Competitive Low Rate on a Mortgage or Refinance.  
Call us at (855) 209-3166.

[START SAVING NOW >>](#)

as of 01:31PM ET 8/5/2013

DJIA	15603.64
	-54.72
NASDAQ	3687.95
	-1.64
S&P500	1705.9
	-3.77

QUOTE:  [GO](#)

strong mobile growth; stock soars 20%



Google ends Chromecast-Netflix promotion 'due to overwhelming demand'

Ads by Google

### Need Insulin Syringes?

All Our Syringes Are On Sale Today. Great Prices, Ships Fast-Shop Now!

[totaldiabetessupply.com/Insulin](http://totaldiabetessupply.com/Insulin)

### Is He Cheating On You?

1) Enter His Email Address 2) See Hidden Pics & Social Profiles Now! [Spokeo.com/Find-Cheaters](http://Spokeo.com/Find-Cheaters)

Chandra McMahon, the chief information security officer for military technology giant Lockheed Martin Corp., said phishing attacks aimed at its employees try to replicate emails and websites of industry organizations that its employees visit on a regular basis.

"They are compromised by adversaries because they are the perfect spot to put malware because a lot of the employees from the industry will go there," McMahon said.

As technology firms find ways to make emails safer for consumers, some security experts suggest treating every link skeptically. So if you can never click on a link in an email again, what options are left? Here are some suggestions from security experts:

- Open links on an email app on Apple Inc.'s iPad or iPhone. These devices have fewer vulnerabilities so malware is unlikely to stick or get attached by clicking on a bad link. Android devices aren't as foolproof, but smartphones certainly have fewer holes than personal computers.

- A few tech companies are promoting a new technology known as Domain-based Message Authentication, Reporting & Conformance, or DMARC, that offers users a visual indication that an email is coming from the legitimate vendor. For example, real emails from EBay Inc. in Gmail include a key next to the "from" field. In Microsoft Corp.'s Outlook, a green key is the sign. Despite a push from firms such as email security provider Agari Data Inc., not every major company has joined this effort.

- Other companies are taking different approaches. Wal-Mart Stores Inc., for one, is devising its own tool. Others are trying to block bad emails from reaching the inbox by harnessing the power of big data to see whether a message has the right context clues, anyone's ever received a similar email or whether the sender's ever been replied to. Technology from Proofpoint rewrites a URL, redirecting users to a cloud-based environment in which the email is opened behind the scenes. If malware is found, the user is blocked from visiting the website.

In essence, Proofpoint Chief Executive Gary Steele said, "we click for you in a sandbox in the sky."

This last approach does raise some privacy concerns, but Steele says all information sent online is encrypted and stored under lock and key. Only the customer has the key, so a judicial body must go to the customer directly to get that key.

With the warnings about these sophisticated and consequential attacks starting to grow, it's possible employees could start facing repercussions for not being cautious with links.

Peter Toren, a former Justice Department computer crimes prosecutor, said he hasn't heard of any companies firing someone for introducing malware into a corporate system by clicking a link. But he said a company might eventually have to make an example of someone.

"They certainly wouldn't sue an employee, because they don't have deep pockets to pay a claim," Toren said. "But it certainly could be grounds for termination. You failed to listen to us. You failed to follow training."

[pares.dave@latimes.com](mailto:pares.dave@latimes.com)

Twitter: @peard33

Copyright © 2013, Los Angeles Times

Comments 5 Email Share 212 Tweet 101 Like 111 7

oil executives and managers at military contractors. The phishers are increasingly trying to get proprietary documents and pass codes to access company and government databases.

Nearly every incident of online espionage in 2012 involved some sort of a phishing attack, according to a survey compiled by Verizon Communications Inc., the nation's largest wireless carrier.

Several recent breaches at financial institutions, media outlets and in the video game industry have started with someone's log-in information being entered on a false website that was linked to in an email.

When an Associated Press staff member received an email in April that appeared to be from a colleague, the individual didn't hesitate to click on the link. But that link led to the installation of a "keylogger" that enabled a hacker to monitor keystrokes and see the password for the Associated Press' Twitter account.

The hacker posted a tweet from the account saying that someone had bombed the White House. As investors reacted to the tweet, the S&P 500 index's value fell \$136 billion. The parody news site the Onion fell prey to a similar, though less costly, attack.

advertisement

## THIS WEEK'S CIRCULARS



See Reduced Prices on Select Sofas at Big Lots! Big Lots



Get the Best in Brand Names at The Sports Authority Sports Authority



Check Out Food Lion's Bakery MVPs Today Food Lion

MORE CIRCULARS >



Predator wasp used to fight citrus disease threat



Injured Afghan girl finds second home in U.S.



TSA misconduct rises; should travelers worry?



Transient held in lethal Venice hit-and-run

Ads by Google



Photos of the Day

More >

Most Viewed Latest News

Anne Globe resigns as DreamWorks Animation marketing chief 08/05/2013, 8:31 a.m.

Venice crash: Autopsy for Italian newlywed

**MORE FROM THE TIMES**

Goldie Hawn and Kurt Russell bail out of their Malibu beach house

Jamie Lee Curtis home, resting after serious car accident in Venice

Goldie Hawn and Kurt Russell bail out of their Malibu beach house

Twelve-year-old contestant feels cheated by 'Jeopardy!'

Simon Cowell baby drama gets more scandalous: Adultery alleged

**FROM AROUND THE WEB**

Bathroom Surfaces Can Be Mold & Mildew-Free with This Simple Solution | *Scotch-Brite*

Lindsay Lohan Before and After Plastic Surgery | *Hollyscoop*

Teen sues school for \$2 million over misuse of Facebook bikini photo | *Digital Trends*

11 Public Universities with the Worst Graduation Rates | *The Fiscal Times*

Finally, One Link Established- Chronic Fatigue Syndrome (CFS), Lupus, Fibromyalgia, Autoimmune disease and Chronic Lyme Disease | *Envita*

planned for Monday 08/05/2013, 8:30 a.m.

Scientists cook, eat beef made from cattle stem cells grown in lab 08/05/2013, 8:29 a.m.

Stocks flounder on a quiet day on Wall Street 08/05/2013, 9:33 a.m.

L.A. Now Live: Latest on Venice boardwalk deadly hit-and-run 08/05/2013, 8:03 a.m.

Recommended by

Ads by Google

**Outlook Support Number**

Call (USA Tollfree) 1-855-888-2803. Support for Outlook issues!  
[Outlook-Support.fixyouremail.com](http://Outlook-Support.fixyouremail.com)

**Have a New Business?**

Start Generating Publicity & Attracting Customers-Join Free!  
[PRWeb.com](http://PRWeb.com)

Comments (5)

[Add](#) / [View comments](#) | [Discussion FAQ](#)

**Archies\_Boy** at 5:50 AM July 27, 2013

Thanks for the heads-up article. When I see such pieces, I send them to all my friends, especially those "of a certain age" who are susceptible to getting scammed. Every little bit helps!

**chastmorris** at 7:49 AM July 26, 2013

The Internet was not designed for general business purposes hence the instability of the system. Once banks joined the fun, the cracks became apparent. It's all Al Gore's fault.

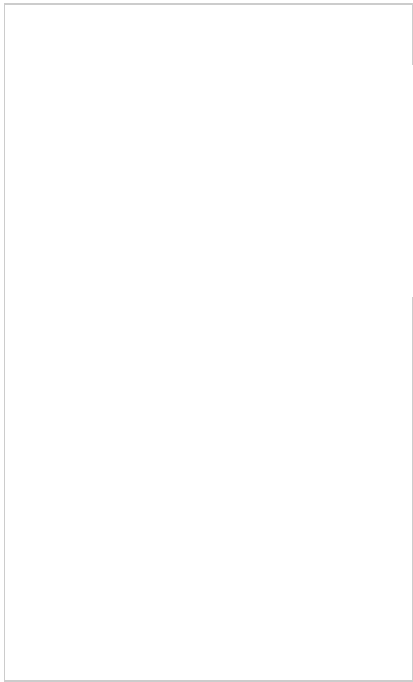
**AdamWickPrk1717** at 7:34 AM July 26, 2013

These cowardly white collar criminals who hide behind computer screens need to be tracked down and thrown in Gen Pop with hardened thugs. I despise computer hackers for all the problems and headaches they cause normal people just trying to do their jobs or browsing the Internet.

*Comments are filtered for language and registration is required. The Times makes no guarantee of comments' factual accuracy. Readers may report inappropriate comments by clicking the Report Abuse link next to a comment. Here are the full [legal terms](#) you agree to by using this comment form.*

Premium content. Unique experiences. Exclusive offers. Only with Membership  **Start now**

**Video**



advertisement

**Save Money**  
Print Coupons from all your favorite brands



Reader Travel Photos »



Share your summer travel photos. We'll publish the best in print and online. [2012 highlights](#)

In Case You Missed It...



**Photos:** Anarchy along Mexico's southern border



**Photos:** Citrus growers import wasp to fight disease



**Photos:** Pedestrians hit on Venice boardwalk



**Photos:** L.A. X Games 2013



**Photos:** Hollywood backlot moments

[Corrections](#)

[Digital Services](#)

[Media Kit](#)

[About Us](#)

[Contact Us](#)

[Site Map](#)

# Los Angeles Times

Burbank Leader | Coastline Pilot | Daily Pilot | Huntington Beach Independent | News Press | Valley Sun | KTLA | Hoy  
Baltimore Sun | Chicago Tribune | Daily Press | Hartford Courant | Los Angeles Times | Orlando Sentinel | Sun Sentinel | The Morning Call  
[Terms of Service](#) | [Privacy Policy](#) | [About Our Ads](#) | Copyright 2013

*A Tribune Newspaper website*