

APRIL 3, 2006

Computer Security

By Brian Grow

Phisher Kings Court Your Trust

Computer-based fraudsters are finding new ways to trick people -- not technology -- to get the information they seek

STORY TOOLS

- ▶ [Printer-Friendly Version](#)
- ▶ [E-Mail This Story](#)
- ▶ [Reader Comments](#)

POLL

INSTANT SURVEY >>

[Google plans to sell 5.3 million more shares.](#) Where should the Web-search company concentrate the additional funds?

- Acquisitions. Let the spending spree begin
- Rely on its own know-how to diversify
- Expand overseas
- Unsure

[VIEW POLL RESULTS >>](#)

PEOPLE SEARCH

Search for business contacts:

First Name :

Last Name :

Company Name :

PREMIUM SEARCH

Search by job title, geography and build a list of executive contacts



Tech White Papers

- ▶ [Most Recent](#)
- ▶ [Most Popular](#)

SPECIAL REPORT

Computer Security>>

- [Phisher Kings Court Your Trust](#)
- [What I Learned at Hacker Camp](#)
- [A Guide to PC Security Products](#)
- [This Worm Is Nasty, Brutish, And Sneaky](#)
- [Stopping a Scam from Spreading](#)
- [Dazed and Confused: Data Law Disarray](#)
- [Gator is Dead. Long Live Claria](#)

"Lawsuit against you," reads the subject line in an e-mail that hit thousands of in-boxes around the world last month. In flawless legalese, the message warns recipients that they recently sent an unsolicited fax to the sender's office. Citing U.S. civil code, its prohibition on sending junk faxes, and an actual \$11 million settlement by restaurant chain Hooters, the missive threatens a lawsuit over the alleged junk fax.

"If you do not pay me \$500 by the deadline for payment, I intend to sue you for violating the Telephone Consumer Protection Act," it reads. "If you force me to sue, I will not settle for less than \$1,000." Details of the alleged lawsuit are contained in the document attached to the e-mail.

In today's litigious -- and digital -- society, being notified of a lawsuit via e-mail might not seem too unusual, right? Gotcha! The e-mail is a scam that preys on deep-seated fears of being hauled into court. Its target: unlucky recipients who may indeed be among thousands of companies that send junk faxes.

SPAM SANDWICH. The attachment -- labeled lawsuit.exe -- is a new variant of a computer worm called Bagle. When worried victims open the attachment, malicious code embedded in its text downloads onto their PCs, and then swiftly harvests all their e-mail addresses to send out even more spam. That second wave uses the victim's personal e-mail address to send malicious code disguised as, say, a Paris Hilton sex video, to friends and associates (see BW Online, 4/10/06, "[This Worm is Nasty, Brutish and Sneaky](#)").

"This is one of the most innovative ideas used by spammers to target unsuspecting users," says Govind Rammurthy, chief executive of computer security firm MicroWorld Technologies, which sent out a warning about the lawsuit.exe scam in March.

As Web-based scams proliferate, it's often psychological cunning, deployed on top of surreptitious code, that is the secret to cyber-criminals' success. Like traditional con men on the street, Internet fraudsters need a never-ending supply of ways to convince victims to trust them -- to open an attachment, click a link, or innocently enter personal data on a Web page.

IN YOUR HEAD. Overpowering instincts, rather than firewalls, is the surest means, say analysts, to pickpocket personal identities and online bank accounts. "You can't install a software patch for a person's mind," says Barry C. Collin, chief executive of cyber-security consulting firm Threat and Risk Associates.

In fact, security analysts say hackers are spending serious effort in researching the psychological vulnerabilities of potential targets. Security firm TrendMicro's director of global education, David Perry, says they watch news headlines for poignant world events and often review the success of an attack by reading press releases and corporate warnings, in order to tweak the next attack for greater effectiveness.

Hackers also look for situations of confusion to exploit, such as a corporate merger. For example, at Vigilar's Intense School in Ft. Lauderdale, FL., where they train people in ethical hacking to help fortify digital defenses, they use a bogus e-mail from someone pretending to be a helpdesk employee trying to verify account data for a database that is being combined in the wake of a merger.

TRUST ME.... "There is a lot of implied trust that you can manufacture -- and exploit," says Ralph Echemendia, an info-tech security instructor at Vigilar's. Echemendia used the 2004 merger of Wachovia and SouthTrust as a model to deploy the script and tap merger chaos.

Analysts say phishing attacks also often spike after a data security breach hits news headlines. The reason: Customers are already anticipating a potential request to update account data and monitor credit reports.

"It makes them more vulnerable to psychological scams," says Herbert H. Thompson, chief executive of Security Innovation.

ONE-TWO PUNCH. Take the case of a phish targeting Citibank customers this year. To build trust, it operates in two phases, say analysts. First, an e-mail purportedly from Citibank warns that customer accounts may have been compromised in a previous scam. But it doesn't ask for personal information.

Instead, the scam requests an e-mail address, just in case the victim's account is found to be hacked. Then, later, a second phish is sent out warning that, indeed, the account has been compromised -- and requests an update of financial details.

"Trust was built in the first step. Then, in the second step, they asked for confidential information," says MicroWorld's Rammurthy, who estimates some 60% of victims who received the second e-mail provided personal and financial data (see BW, 1/9/06, "[Gold Rush](#)").

Indeed, with overall returns from phishing attacks falling, Web criminals are succeeding in finding novel new ways to convince users to open documents or click links that download data-stealing software onto PCs. Instead of directly asking the user to enter personal data into a fake Web site, cyber-criminals are embedding code into fake news articles or business-oriented "requests for proposals" which, when opened, install a backdoor into the PC, then log keystrokes. Russian security firm Kaspersky Lab estimates the use of data-stealing code designed specifically to steal financial information, known as Trojans, rose 402% in 2005.

SHARING THE STEALTH. The upshot: Fewer people are, themselves, coughing up personal info, but fraud losses continue to climb. A 2005 survey by Gartner found that just 2.5% of phish recipients responded with personal or financial information, down from 3% in 2004. But fraud losses connected to the theft of such information off the Web still rose from \$690 million in 2004 to \$1.5 billion last year. "If I'm a scammer, I have to do something that will make you trust me," says John Pescatore, senior vice-president of Internet security at Gartner.

Law enforcement agents say that while the thinking behind cyber-scams is not much more complex than age-old cons run by offline grifters, it's clear cyber-criminals are pooling their brainpower to devise new techniques. A DVD available in foreign black markets called "Hacker's Handbook" contains scores of tips on how to trick victims, according to Trend Micro's Perry.

Former hacker Kevin Mitnick, who now runs his own security consulting firm, hosts a two-day "social engineering" conference for clients that includes sessions entitled "Bugs in the Human Hardware." At hacker sites such as mazafaka.ru and astalavista.box.sk, criminals often share ideas on how, for example, to exploit new state laws in the U.S. requiring firms to issue warnings when customer databases have been hacked.

ROYAL SCAM. Some scam artists still plot the old-fashioned way: by holding physical court. Law enforcement agents say Nigerian fraudsters often gather in Internet cafes in the country's capital, Lagos, to concoct the newest bait.

Famous for pioneering so-called 419 letters -- pleading e-mails from bogus foreign businessmen seeking to move money out of their country by tapping U.S. victims' bank accounts -- the Nigerian scammers are now establishing romantic relationships in online dating Web sites in order to dupe lonely love interests into giving up financial information.

"It's group brainstorm," says Gregory S. Crabb, a senior investigator for the U.S. Postal Inspection Service in Washington, D.C., who has hunted cyber-criminals around the world. (see BW Online, 5/30/05, "[Hacker Hunters](#)").

CHEAP THRILLS. Hackers are even finding ways to take the pain out of writing malicious code, a move that may enable more concentration on upgrading the psychology of the cyber-scam. On Mar. 24, security firm Sophos said it had discovered a Russian Web site selling a spyware kit called WebAttacker for less than \$20. The pre-fab software downloads a program that tries to turn off PC firewalls, then installs a keystroke-logging device.

Already, it has been spammed-out via e-mail touting news stories about bird flu and the recent death of ex-president of Serbia, Slobodan Milosevic. The technical skills required to be a cyber-criminal have been removed as an entry-level barrier. "In order for the cyber-crime business to continue, it is going to rely more and more on social engineering," says Ron O'Brien, senior security analyst at Sophos.


[Grow](#) is a correspondent in *BusinessWeek's* Atlanta bureau

READER COMMENTS

BW MALL SPONSORED LINKS

- [Enterprise-Grade Link Failover and Load Balancer](#) Easy to install. Fully transparent to existing firewall and router. PePLink Balance offers link failover and load balancing for branch office networks. Supports DSL, T1, Wireless & Cable. Centralized Configuration, Management and Traffic Reporting.
- [Prove Advertising ROI: 100% Accurate Call Tracking](#) CallSource tracks over 100,000 advertising sources with unique toll-free and local numbers. Detailed reports are delivered by web, email, FTP and XML. Track all ad sources to calculate ROI --online and off.
- [NetSupport DNA - IT Asset Management Software](#) Facing compliance issues? Manage your IT assets. Track and monitor software and hardware inventory, distribute software, manage licenses, monitor Web usage, pull graphical reports, web based helpdesk, remote control and more. Free trial.

- [Order electronics direct from Polaroid](#) Businesses receive preferred pricing and other benefits for volume orders direct from Polaroid. LCDs, branding items, document photography and many more solutions for your business.
- [Attach Plus, makes email encryption second nature](#) Attach Plus adds powerful encryption to your e-mail attach button. Easy-to-use program for encrypting documents sent as e-mail attachments. Attach Plus uses the 128-bit PDF and ZIP encryption. Simplicity; encrypting documents becomes second nature.
[Buy a link now!](#)

Get BusinessWeek directly on your desktop with our [RSS feeds](#). 

Add BusinessWeek news to your Web site with our [headline feed](#).

Click to buy an [e-print or reprint](#) of a *BusinessWeek* or BusinessWeek Online story or video.

To subscribe online to *BusinessWeek* magazine, please [click here](#).

Learn more, go to the [BusinessWeekOnline home page](#)

 [BACK TO TOP](#)

[Advertising](#) | [Special Sections](#) | [MarketPlace](#) | [Knowledge Centers](#)

[Terms of Use](#) | [Privacy Notice](#) | [Ethics Code](#) | [Contact Us](#)

The McGraw-Hill Companies

Copyright 2000- 2006 by The McGraw-Hill Companies Inc.
All rights reserved.

TODAY'S MOST POPULAR STORIES

1. [Next-Gen DVDs' Blurry Picture](#)
2. [A Revolution in Swede Speed](#)
3. [Facebook's on the Block](#)
4. [The Word in Hollywood, "Download"](#)
5. [Nokia's \(Slightly\) Better Cell Phones](#)

[Get Free RSS Feed >>](#)

MARKET INFO

[DJIA](#) 11109.32 -41.40
[S&P 500](#) 1294.82 -5.43
[Nasdaq](#) 2339.79 -1.03

[GO](#)

[Stocks Slip, But Finish Strong for the Quarter](#)

[Create / Check Portfolio](#)

[Launch Popup Ticker](#)

PREMIUM CONTENT

[MBA Insider](#)

BW MAGAZINE

[Get Four Free Issues](#)

[Register](#)

[Subscribe](#)

[Customer Service](#)

ONLINE FEATURES

- [Book Reviews](#)
- [BW Video](#)
- [Columnists](#)
- [Interactive Gallery](#)
- [Newsletters](#)
- [Past Covers](#)
- [Philanthropy](#)
- [Podcasts](#)
- [Special Reports](#)

BLOGS

- [Auto Beat](#)
- [Blogspotting](#)
- [Brand New Day](#)
- [Byte of the Apple](#)
- [Deal Flow](#)
- [Economics Unbound](#)
- [Fine On Media](#)
- [Hot Property](#)
- [Investing Insights](#)
- [New Tech in Asia](#)
- [NussbaumOnDesign](#)
- [Tech Beat](#)
- [Working Parents](#)

TECHNOLOGY

- [J.D. Power Ratings](#)
- [Product Reviews](#)
- [Tech Stats](#)
- [Wildstrom: Tech Maven](#)

AUTOS

- [Home Page](#)
- [Auto Reviews](#)
- [Classic Cars](#)
- [Car Care & Safety](#)
- [Hybrids](#)

INNOVATION & DESIGN

- [Home Page](#)
- [Architecture](#)
- [Brand Equity](#)
- [Auto Design](#)
- [Game Room](#)

SMALLBIZ

- [Smart Answers](#)
- [Success Stories](#)
- [Today's Tip](#)

INVESTING

- [Investing: Europe](#)
- [Annual Reports](#)
- [BW 50](#)
- [S&P Picks & Pans](#)
- [Stock Screeners](#)
- [Free S&P Stock Report](#)

SCOREBOARDS

[Mutual Funds](#)

[Info Tech 100](#)

[S&P 500](#)

[B-SCHOOLS](#)

[MBA Blogs](#)

[MBA Profiles](#)

[MBA Rankings](#)

[Who's Hiring Grads](#)

BW EXTRAS

[BW Digital](#)

[BW Mobile](#)

[BW Online Alerts](#)

[Dashboard Widgets](#)

[Podcasts](#) 

[RSS Feeds](#) 

[Reprints/Permissions](#)

[Conferences](#)

[Investor Workshops](#)

[Research Services](#)
