



Attack of the DOPPELGANGERS

By Carr, Matthew

Publication: [Business Credit](#)

Date: [Sunday, June 1 2008](#)

You are viewing page 1

HEADNOTE

Anyone who has an email account is no stranger to phishing, spoofing and pharming scams. Both personal and business emails are bombarded with spam trying to sell everything from enhancements, to discount Viagra, medications, printer cartridges, various forms of adult-entertainment, employment opportunities and anything and everything beyond. Technological advances have revitalized many age-old scams and have made them more successful simply because of the sheer number of individuals that can be targeted with the least amount of effort.

IMAGE ILLUSTRATION₁

Today, scammers can send an email to 500 different people with a single push of a button, completely eliminating the exhausting and time consuming process of making 500 phone calls or mailing 500 letters. And, just as with any mass marketing approach, a single response is usually enough to more than pay for the time, materials and effort put in.

"Those who know how to make an email look like it came from a fellow employee will put a virus/Trojan horse on your computer," warned John Tzanis, BA, JD, Continental Legal Services Corporation. "They'll use a key logger to get your password and then you and your company are vulnerable to attack or loss of personal and business information."

Though our modern age has made it prolific, identity theft is also nothing new. It has only been transformed by the distance by which a perpetrator may carry out an attack, with email placing nearly everyone on the planet at some sort of risk, as again evidenced by the proliferation of spam. In the United States, cyber crimes have emerged as one of the fastest growing arenas for law enforcement focus, with a prominence only behind terrorism and foreign intelligence. It is estimated that a person's identity is stolen once every 10 seconds, while globally, nearly 10 million people each year have their identities hijacked. A study by the Aberdeen Group estimated that \$221 billion is lost by businesses worldwide because of these thefts, as victims aren't held responsible for their doppelgangers' actions.

As the world continues to conduct business more and more by electronic communication, there is a growing concern of theft of a corporation's or business' identity and the prevalence of fraud. All companies, small and large, are at risk of being targets or of having their identity stolen. In the end, not only is there the reputational damage caused to a company by scams committed in a company's name, but there are real monetary losses due to fraudulent transactions by those who are victims.

A Case Study: WESCO Distribution

In 1922, Westinghouse Electric Company created WESCO to sell and distribute its growing catalog of products. The organization flourished and in 1994, the management team of WESCO, in partnership with the private investment company Clayton, Dubilier & Rice, purchased WESCO from Westinghouse. The holding company WESCO International was formed following another purchase in 1998 and went public on the New York Stock Exchange in May 1999. It is a Fortune 500 success with more than \$5 billion in annual sales, 7,000 employees in 400 full-service centers and over 110,000 customers around the globe.

But in July 2006, an individual claiming to be the manager of WESCO's Cleveland, OH branch began placing purchase orders with several computer distributors for seemingly innocuous items such as toner, ink cartridges and computer memory sticks. The distributors took the orders and began sending invoices to the Cleveland branch, which then forwarded them on to corporate.

"That's basically how it started," said William Coe, asset protection manager, WESCO. "We initially thought, as I started the investigation, that it was an isolated incident; that

somebody was impersonating this branch manager in the Cleveland area. I had no idea that it had far-reaching implications into international areas."

Shortly after, a similar situation came to light as someone posing as WESCO's chief executive officer (CEO) began submitting purchase orders for the same items. They'd place an order for several thousand dollars and ask for a line of credit. Almost all of the transactions took place over the Internet and the sales people for the distributors failed to place a single phone call to verify any of the information or authority. The emails from the individual claiming to be WESCO's CEO and others arrogantly provided a series of phone numbers, knowing that if any of these were dialed, they would have been found out to be fictitious or disconnected.

In trying to convince law enforcement to take up the case, WESCO found itself in a strange situation as it wasn't a victim in the classic sense; the company wasn't suffering a loss. It was the third party suppliers that were targeted and faced the loss of tens of thousands of dollars.

"Legally, WESCO did not suffer a monetary loss," stated Coe. "The biggest problem we had was that because we are publicly traded, our reputation was at stake. We could ill afford to have the Wall Street analysts or others start bad-mouthing WESCO for being mixed up in some type of scam. That's one of the reasons why we started collecting all this data and contacting the U.S. Secret Service once we found out it was a large operation that was organized and really targeting hundreds of companies. They targeted everyone from Dells to HPs down to the mom-and-pops running out of their garage."

Simplicity and Villainy

The total number of companies contacted by fraudsters portraying as WESCO representatives cannot be determined during the period of July 2006 and the end of 2007; however, WESCO received at least 1,500 calls from companies during that same period. The assault isn't slowing, as just in the first quarter of this year, another 200 companies have contacted WESCO reporting they had received fraudulent purchase orders in the company's name.

The approach the scammers have used is simple, yet elegant. It also clearly demonstrates that, even though there are countless warnings about email scams, there is still a broad naïve base out there for criminals to readily and successfully prey upon.

The perpetrators would pose as anything from a corporate executive at WESCO, to a purchasing agent, to one of the company's 400 branch managers. The vast majority of the contact was done via email, originating from addresses that had WESCO somewhere in the name. Coe has collected more than 40 different email addresses and at least two dozen different individuals for whom the scammers have posed. In some cases it was a genuine person, like the CEO, CFO or a number of other executives, or it would be a common name plucked from the air that by chance matched someone from WESCO's large employee base.

"Our previous email address was _____@wescodist.com. The fraudsters would use wescodistr.com or they might have wescodists.com or wescocompany.com," explained Coe. "It's just a little variation. Then it started appearing as the first part of the address, like wescosales@earthlink.net or wescoppm@gmail.com. So, they started using all sorts of free email providers like Yahoo!, EarthLink, NetZero and so on."

Even more devious was that the perpetrators also began contacting distributors using TTY/TDD telephones for the hearing impaired. The service is toll-free and uses an operator to relay responses between a hearing-impaired person and another party by reading aloud what was typed by the hearing-impaired individual and then by typing what was said by the other party. This allowed the perpetrators to hide their voices, improper grammar and misspelled words.

The basic scenario consisted of the fraudsters asking for a quote on first contact, and once that was received, they would come back with a purchase order. The purchase order, a fairly uniform document, would be legitimate looking enough, including a WESCO logo that had been extracted from one of the company's websites and placed in the letterhead to make it look more official. When the fraudulent purchase order was sent, it was typically between \$30,000 and \$60,000 and asked for net 30 terms. On a few occasions, multiple stolen credit cards were used to pay for the order, but most of the time they were given some kind of a line of credit. If a credit application was sent to be filled out, the information was readily available. Since WESCO is a publicly traded company, the pertinent information could be gathered through one of the company's websites or through its prospectus.

"They tried to target salesmen versus management... to dangle that nice commission for that guy out there," said Coe. "Once they got that initial purchase, it would quickly be followed by

several other purchases of equal or greater value, but it would be the same type of items- almost identical. They would try to instill a sense of urgency by insisting that they needed the items yesterday and that they needed them shipped overnight to a particular address.

Basically, they didn't care how much it would cost for them to ship it." Coe added, "They were counting on a degree of greed from the commissioned sales person and then they were also counting on this sense of urgency to keep that sales person from practicing due diligence."

To add to the convincing scheme, the fraudsters were armed with WESCO's Dun & Bradstreet number, which is also readily available, as well as some of WESCO's references. "The problem is some of the suppliers dealing with us on a regular basis would naturally send the products out," stated Coe. "They would not question it because we had already established lines of credit." Unfortunately, the lack of followthrough has cost some of the duped companies as much as \$750,000, the result of a single salesman who hurriedly sent out product in anticipation of a big commission.

As usual, there were plenty of warning signs, that were simply ignored. As Coe related, "The dollar tends to blind individuals to some of these obvious red flags." For example, after submitting an order, the fraudsters would provide a point of contact which was usually a residential address somewhere in the United States. And in every single case, the address was different than where the person making the call was supposedly located.

The sad truth is that the individuals that lived in the homes that these items were being shipped to were victims themselves. In some cases, they had met the criminals online in a chat room or some other virtual venue and had fallen hi love with them. The fraudsters said that they needed a favor, and the lovestruck individuals readily accepted. The perpetrators found others by trolling job search sites and, knowing these people were in need of work, asked if they would like a position with WESCO as a freight forwarder. The job was easy enough: the individuals could work from home accepting deliveries and all they had to do was re-label the boxes to have them shipped outside of the country. The fraudsters even got these people to pay for the overseas shipping charges out of their own pockets with the promise that any money spent would be reimbursed. A little while back, WESCO had a series of checks sent out to suppliers stolen in transit. These were reproduced in a variety of different forms, and even sent as paychecks, just like those of WESCO employees, to these duped "freight forwarders." Unfortunately, 10 to 12 days later, the bank would come back and

inform them that the check was fictitious. But by then it was too late, the fraudsters had gotten to use these individuals and their homes for close to 40 days, with shipments arriving and being sent overnight. They had already moved on to their next victim.

"There were no arrests on these people because they were basically unaware of what they were doing," recounted Coe. The freight forwarders shipped the boxes to a legitimate importer/exporter in the United Kingdom, who then forwarded them on to Nigeria. From Nigeria, many of items like toner and ink cartridges, since they don't have serial numbers and are readily disposable, made their way back into the U.S. via Canada and Mexico and have been reportedly sold at discount outlets. Computer supplies and peripherals aren't the only items to have been targeted though. Larger ticket items, like earth-moving equipment from Caterpillar, diesel engines and diesel engine parts suppliers and LCD projectors, have also been scammed.

Even WESCO itself has been a victim. A company that WESCO purchased was contacted by the fraudsters with the standard script. In an act of overzealousness and wanting to show the new parent company that they could ship with the best of them, this newly-acquired company shipped over \$100,000 worth of product to the criminals. Fortunately, this worked to WESCO's advantage, to a degree. Since the company had all the tracking information, the U.S. secret Service was able to trace the merchandise to locations in Washington State and Florida, where it had been forwarded to London. In London, the secret Service had a detachment that went to the importer/exporter and located some of the boxes. Others had already been sent on to Nigeria. A short time after that, Nigerian authorities made two arrests of Nigerian nationals and confiscated tens of thousands of dollars worth of merchandise. The two men are still incarcerated in Nigeria.

Even more frustrating than its name being blighted, said Coe, is that WESCO has now become a mark. "The thing that I am more concerned about than anything else, and we've found this in the past couple weeks, is that now we're seeing evidence that the fraudsters are impersonating other large companies and using their identities to target WESCO," explained Coe. "We've put out several fraud alerts to our people because I knew the other shoe was going to drop; it was just a matter of time before we would be a target."

Lessons Learned

The WESCO case, which is just one of a seemingly growing number, shows that there has to be greater due diligence on the part of everyone, and most importantly sales staff. The Federal Trade Commission and the secret Service do not keep statistics on how many companies are affected each year by these attacks, or how much money is ultimately lost. WESCO alone has had nearly 2,000 companies report receiving fraudulent purchase orders in its name. The company made a bold move by posting a security caution on its website informing any company that if there's even the slightest bit of suspicion about an order, to contact the company directly via telephone.

"I think that in putting something like that on our website shows we are concerned, not only about our business and our reputation, but also in trying to protect the public and our fellow distributors," said Coe.

The larger issue is how easily the fraudsters are able to perpetrate these scams and often how easily some individuals are fooled. "I could register www.cocacolorp.com today, create a fake website and offer you a free case of Coke if you go to my website and give me personal information," said Tzanis. "I am sure it happens everyday via spam emails. But I doubt that spammers are specifically targeting companies that often. They will take what they can get."

Tzanis relayed information easily obtained from a public website that provided instructions on how to "spoof" emails and pose as an employee of a company. It also demonstrated how shockingly simple it was to perpetrate with even modest computer skills. "In the WESCO case, that person could have actually used the president's email address to send those 'spoofing' orders," explained Tzanis.

The onus is on all staff members to be vigilant.

"You really can't prevent this from happening. The only thing you can do is the security caution, which we did eventually," Coe said. When your company is a publicly traded Fortune 500, your company's information is out there, you can't prevent that and you can't prevent ID theft. "It's almost impossible," Coe said. "And it's not until you start getting the invoices or you start getting queries from third parties do you know that it's even occurring."

Legally, it's a difficult situation when a company's name is being used to defraud others. Enforcement oftentimes builds a case on substantiated loss. WESCO had to convince the secret Service that the fraud posed a potential loss of reputation, which could be even more

damaging in the long run. "Reputational damage is long-lasting," stated Coe. "Thousands of dollars in a loss is nothing versus the millions lost in a down tick of stock prices that can decimate a company."

Credit and sales staff can have a variety of tools available to them. If an email with a suspicious originating web address is received, a simple search on registration sites like GoDaddy.com or a "Who Is" search on NetworkSolutions.com will tell when a web address was registered, who the administrator is and where they're located. "Practice a modest amount of due diligence," recommended Tzanis. "Just run the address; just run the phone number. If you Google either and they're supposed to be from a well-known company but there's no match, then it's probably a scam."

"The first point is that if it sounds too good to be true, it probably is," added Coe. "I don't know if we'll ever be able to prevent it from happening. I think it's going to be a more of an educational-type of thing on the part of the potential victims. They are the ones that are going to have to look out for themselves, because it's going to happen and it continues to happen."

SIDEBAR

"Now we're seeing evidence that the fraudsters are impersonating other large companies and using their identities to target WESCO, explained Coe.

SIDEBAR

"I could register www.cocacolorp.com today, create a fake website and offer you a free case of Coke if you go to my website and give me personal information," said Tzanis.

SIDEBAR

"Practice a modest amount of due diligence," recommended Tzanis. "Just run the address. Just run the phone number. If you Google either and they're supposed to be from a well-known company but there's no match, then it's probably a scam."

SIDEBAR

WESCO's Checklist

Here are some red flags Coe and WESCO developed and use routinely to help the company's staff be proactive against fraud. It's something Coe suggests other companies should, and continue to, instill.

- * The sender's email uses a generic service rather than a company name
- * Large quantities of the same item are ordered
- * The shipping address given differs from the company's actual address
- * The language used in the emails is flawed, consistently misspelled and reads like it's been translated from another language
- * Multiple credit cards are used for the purchase
- * They attempt to get net 30 terms
- * An alternative shipping method faster than typical mail is requested, such as overnight air
- * Multiple rush orders are received from the same company in a short period of time

AUTHOR_AFFILIATION

Matthew Carr can be reached at matte@nacm.org.

[1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) [Next Page](#) ▶

In addition, make sure to read these articles:

- [AT&T Inc to use McAfee's anti-spam technology.](#)
- ['Phishing' Attack Puts Hook in Cox](#)
- [Zone Labs launches new ZoneAlarm Security Suite.](#)
- [Zone Labs launches new ZoneAlarm Security Suite.](#)
- [A safer model for online job sites?](#)
- [Evolving Endpoint Security](#)

Sponsored Results

- [Identity Theft Protection: As Seen on TV](#)
- [Identity Theft Response Call Center Services](#)
- [Life Lock Identity Theft Prevention and Credit Protection](#)



Related Resources

Press Releases

- [MX Logic Selected to Protect PETRO Holdings against Spam, Email Threats; Home Heating Oil Distributor Realizes Multiple Benefits of Fully Managed Email Defense.](#)

DENVER -- MX Logic Inc., a provider of innovative, easy-to-use email defense solutions to businesses of all sizes, today announced that PETRO Holdings, the

- [Korean Realtor Empowers Real-time Business with Juniper Networks.](#)

Kyobo Realco Secures Nationwide Distributed Enterprise by Deploying High-Performance Secure Services Gateway and NetScreen Appliances SUNNYVALE, Calif. -- Juniper Networks, Inc. (NASDAQ:JNPR), the leader

- [Cartoon Network Joins Forces with Outblaze inAsia.](#)

Alliance to Develop New Media Offerings That Keep Young Consumers Engaged RIVERSIDE, Conn. -- Outblaze (www.outblaze.com), the world's largest online service platform providing white label

Latest Posts



[Cyber Crime Part II: How to Protect Your Company from BrandJackers](#)

The broad spectrum of brandjacking covers activities like bidding on a brand's keyword within a search platform, using a brand's logo to deceive site visitors ...

[Read More](#)



[The Business of Being a Scumbag, Part II](#)

The Business of Being a Scumbag, Part II From today's Direct Newsline email newsletter (no apparent way to link to it) comes another view ...

[Read More](#)



[Cyber Crime Part II: How to Protect Your Company from BrandJackers](#)

The broad spectrum of brandjacking covers activities like bidding on a brand's keyword within a search platform, using a brand's logo to deceive site visitors ...

[Read More](#)

Podcasts

- [How to Protect Your Customers from Identity Theft](#)

Allbusiness.com's Paul Kilduff interviews Joanna Medin, a specialist in helping small businesses set up procedures to stop identity theft.

- [How to Design an E-Mail Newsletter to Maximize Your ROI: Part 1](#)

AllBusiness.com's Chris Bjorklund interviews Joseph Carrabis, the founder of Next Stage Evolution, on what works and what doesn't in e-mail newsletter design.

Premium Content

- [In Phishing, Legitimate-Looking E-Mails, Web Sites Trick, Steal from Consumers.](#) 💰

By Jonathan D. Epstein, The Buffalo News, N.Y. Knight Ridder/Tribune Business News Apr. 12--Gone "phishing" lately? No, it's not a misspelling. It's a growing global ...

- [Fleet Bank Customers Join Preferred Prey of E-scammers.](#) 💰

By Timothy C. Barmann, Providence Journal, R.I. Knight Ridder/Tribune Business News Apr. 27--Fleet Bank customers are being targeted by nearly two-dozen Internet scams designed to ...

Forms and Agreements

- [Agreement and Plan of Reorganization between Ask Jeeves Inc. and Interactive Search Holdings](#)
- [Agreement and Plan of Merger between Intermix Media/ MySpace, Fox Interactive Media, Inc. and News Corporation](#)
- [All Forms](#)

Ads by Google

[Criminal Defence Lawyer](#)

Your best defence. Call now for a free consultation. (647) 330-3201
www.defendme.ca

[Personal Injury Law](#)

Injured? Know Your Rights! Free Case Evaluation by a Lawyer
www.pilco.ca

[Traffic Ticket? Impaired?](#)

Expert defense in Southern Ontario for over 20 years by an ex-copper.
www.mathesons.ca

[Free Border Evaluation](#)

3 Million Canadians are ineligible to enter the U.S. Are you one?
www.canadianpardons.ca

Business Resources

- [Vendor Quotes](#)
- [Business Directory](#)
- [Office Products](#)
- [Free Business Magazines](#)
- [Franchise Opportunities](#)

Sponsored Links

[AllBusiness Business Directory](#)

Find product and service providers in over 65,000 categories

www.allbusiness.com

[Business Purchases Quote Center](#)

Get fast, free competitive quotes on business purchases from qualified vendors

allbusiness.vendorseek.com

[Search for jobs on AllBusiness](#)

Search millions of jobs from across the web

www.allbusiness.com

[Site Map](#) | [Contact Us](#) | [FAQs](#) | [About Us](#) | [Media Kit](#) | [Reprints](#) | [RSS Directory](#) | [Sign Up for Free Newsletters](#) | [Disclosure Policy](#)

Copyright © 1999 - 2008 AllBusiness.com, Inc. All rights reserved.

No part of this content or the data or information included therein may be reproduced, republished or redistributed without the prior written consent of AllBusiness.com.

Use of this site is governed by our [Copyright and Intellectual Property Policy](#), [Terms of Use Agreement](#) and [Privacy Policy](#).

© Copyright National Association of Credit Management Jun 2008

Provided by ProQuest, LLC. All rights Reserved.

You may not repost, republish, reproduce, package and/or redistribute the content of this page, in whole or in part, without the written permission of the copyright holder.

[Get In-Depth Company Information from Hoover's](#) | [Buy a D&B Credit Report](#) | [What is in Your Company's D&B Credit Report?](#) | [Article Archives](#)

[Online Business Database](#) | [Online Business Information](#) | [Email Marketing Lists](#) | [Sales and Marketing Solutions](#) | [Business Mailing Lists](#)

Information and opinions on AllBusiness.com solely represent the thoughts and opinions of the authors and are not endorsed by, or reflect the beliefs of,

AllBusiness.com, its parent company D&B, and its affiliates.

