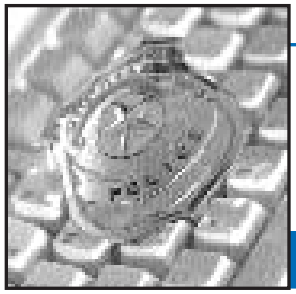
Volume 3 No. 1 January 2004



CYBER-CRIME FIGHTER

SUCCESS SECRETS FOR SECURITY MANAGERS AND INVESTIGATORS

IN THE NEWS

InfoSec: Real Progress… Or Just a False Sense of Well-Being?

Most information security professionals accept that their organizations are at risk for a major cyber attack. But nearly 80% of them are confident that they're prepared to defend against intrusions.

These are among the results of a survey the Business Software Alliance (BSA) and the Information Systems Security Association (ISSA).

The survey was conducted by doing on-line interviews of 1,716 ISSA members.

Caution: While this high level of security confidence sounds encouraging, it does not account for what some respected infosec analysts consider to be inadequate attention to hardening operating systems to keep their systems safe.

Also worrisome: The continued shortage of investment in employee security awareness and training. Industry analysts agree that without thorough and continuous training, real information security is unattainable.

***Cyber-Crime Fighter* sources:**

- *BSA-ISSA Information Security Study: Online Survey of ISSA Members,* http://global.bsa.org/policyres/BSA-ISSAsurvey.pdfhttp://global.bsa.org/policyres/BSA-ISSAsurvey.pdf
- Prominent information security experts who requested anonymity.

IN THIS ISSUE

Mark W. Ishman, Esq., *Triangle Law Center, PLLC*

MINIMIZING THE RISK OF ON-LINE FRAUD

What Credit Card Companies Don't Want You to Know

Actual Web bulletin board posting: *Hey, I've been carding three months but only for amounts up to $500. The holiday season is here and everyone is starting Xmas shopping early and I think this would be the best time to try carding higher amounts. I get cc#s, cvv, addressees and everything needed from my job. I have some ssns and DL#s too. Anything a sales rep could possibly ask for, I have a "legitimate" answer to give. I've thought everything inside-out and outside-in. When I go to card something I have everything written down step-by-step, and I always tell the sales rep the REAL phone# of the REAL cardholder but then I say that I'm visiting my "sister's" house (which is my drop site) and they should call me at her # (which is a pay phone) if necessary. I go to great lengths finding perfect drop sites. My drop sites are always upper-class neighborhoods.*

The reason why I'm posting this is to ask the more experienced carders what they think of carding say $1,000 or even higher? Seriously, if I have ALL the critical info at hand, why couldn't I card a $2,000 laptop computer for myself, or a $1,500 gold necklace to either keep, pawn or maybe sell on ebay?

Does this posting from a carder—someone who steals credit card numbers—scare you? If you are an E-merchant, it definitely should.

STILL NOT WORRIED?

Gartner Inc. estimated that US E-merchants lost nearly $500 million to fraud and potential sales during the 2002 holiday shopping season. Though the 2003 holiday season may be over, the statistics still paint a disturbing picture of why E-merchants must ensure that they are doing everything they can—year round—to avoid being victims of E-commerce fraud.

To succeed, you'll need some basic information about how carders and cyber-shoplifters operate. With that knowledge, you'll be well equipped to implement effective anti-fraud policies and procedures within your E-business.

THE CARDER'S M.O...

•Picking a drop site. Carders always find a drop site before they do the crime. It's a place to ship merchandise they receive via E-fraud. They usually look for drop sites within one to five miles of their residence.

Preferred: Abandoned houses with For Sale signs in front. The carder removes the For Sale sign on the day of delivery and acts as the home owner when the delivery truck arrives.

Self-defense: Most homes that are for sale are listed on an MLS directory. Before shipping, search the local MLS database to see if the shipping address is a home that's on the market.

Variations: Some carders choose a drop site in a wealthy neighborhood and arrange for the merchandise to be shipped when the occupants have left for work or school. Or—they'll choose a drop site on a busy city street where home owners often gather in front of their homes.

Self-defense: Never ship to an address that is not verified by the credit card company as the cardholder's billing residence.

•Placing the order. Carders are very

"smooth" on the phone and have answers to all of the typical authentication questions. When employees speak with customers to authenticate transactions they must be alert to situations where the answers given do not match the data of the credit card company. When that occurs, the employee must immediately report potential fraudulent activity to the credit card company and decline the order.

•**Picking up the package.** After carders have targeted their drop-off site, they will be at that site waiting for the delivery of the merchandise.

Self-defense: Always require a signature for products delivered. If you ever receive a chargeback, whether from a carder or so-called cyber-shoplifters (see below), and you are able to successfully reverse it, you must have a signed delivery slip. This slip will also assist federal and state authorities in prosecuting the carder.

CYBER-SHOPLIFTERS

Cyber-shoplifting occurs when cardholders purchase products or services from E-merchants with a credit card, and after receiving the delivered goods or services, revoke the order or initiate a chargeback for phony reasons.

Result: The credit card company debits the E-merchant's account for the sale and shipping charge and tacks on a chargeback fee. Naturally, cyber-shoplifters never return the rejected goods or services to the E-merchant. So, at the end of the day, E-merchants not only lose the sale and shipping revenue but also absorb a chargeback fee and lose their merchandise.

READ THE FINE PRINT

Your on-line merchant agreement explains when a credit card company can impose a chargeback fee to your account. Unfortunately, too many merchants don't pay enough attention to these terms and end up suffering fraud-related charges that they shouldn't. *Typically a fee may be debited when…*

•The credit card was not presented, the cardholder denies making the purchase and the merchandise was sent to an address other than that of the cardholder.

•Goods or services are either returned or never received.

• Authorization was required but not obtained.

• The sale date is after the credit card's expiration date.

• The merchant received notice that the credit card is not to be honored.

• A sales draft is executed or accepted fraudulently.

•The merchant fails to respond to the transaction processor's requests for additional information about a transaction.

•The cardholder disputes the sale of goods or services, or execution of the sales draft or claims that the sale price is subject to a discount, defense or counterclaim.

MINIMIZING RISK

To minimize chargebacks and fraud losses, enforce strict internal policies and procedures, and follow the defensive measures and procedures outlined above. *Additional important anti-fraud procedures include…*

•Use only third-party credit card authentication services that screen for potential fraud and suspicious transactions, including real-time checks identifying fraudulent activity based on patterns of fraud.

•Manually review each order and decline orders where a customer fails to provide complete information, including credit card number, expiration date, CVV2/CVC2 numbers, cardholder verification, IP address of the order, mailing address, telephone numbers and E-mail address. (See also page 4.)

•Decline orders if the credit card company cannot verify the cardholder's address (AVS). While you're on the phone with the card company, be sure to ask if the credit card is stolen or whether it has had previous fraudulent activity. Most card companies won't tell you this unless you ask!

•Decline orders from free, Web-based or E-mail forwarding addresses. You need to be able to trace the domain back to a real person.

•Decline credit card orders from overseas. You have limited recourse if you are a victim of fraud overseas. Require such cus-

Continued on page 3

If It's Wednesday… The Worm Should Be Dead

The devastating Sobig.F worm that first reared its ugly code in August 2003 was programmed to shut itself down on September 10.

Trap: Computers set to the wrong date remain vulnerable to the worm. While networked PCs are typically set to the correct time and date from a central server, laptops and home PCs often run with the wrong date. Users should periodically check the date on their machines, especially if they are re-booting a laptop after the battery has died.

***Cyber-Crime Fighter* source:**

Paul Wood, principal information security analyst at MessageLabs, www.messagelabs.com, quoted at ZDNet, www.zdnet.com.

CYBER-CRIME FIGHTER

Success Secrets for Security Managers and Investigators

Editor
Peter Goldmann

Managing Editor
Juliann Lutinski

Senior Contributing Editor
Linda Stockman-Vines

Associate Editor
Barbara Wohler

Design & Art Direction
Ray Holland, Holland Design & Publishing

Cyber-Crime Fighter (ISSN1540-0891) is published monthly by White-Collar Crime 101 LLC, 213 Ramapoo Rd., Ridgefield, CT 06877. www.cybercrimefighter.net. Subscription cost: $375/yr. Overseas: $397/yr.

Mission Statement

Cyber-Crime Fighter provides information of maximum practical value to the community of organizations and individuals involved in preventing, detecting, investigating and prosecuting crimes committed by or against computers, networks and individuals.

This community includes law enforcement officials and regulatory officers at all levels of government, corporate security managers, business owners and managers, training professionals and educators.

The editors of *Cyber-Crime Fighter* gather and compile only the *most useful*, authoritative and timely information on all of the many facets of computer and Internet crime.

Comments, suggestions and questions are welcome. Please call us at 1-800-440-2261…or fax to 203-431-6054, or E-mail us at editor@cybercrimefighter.net.

Continued from page 2

tomers to pay via wire transfer or certified bank check.

•Initiate chargeback recovery to get money back from the card company that it wrongly charged back to you.

•Join an E-commerce merchant group to stay on top of the latest credit card scams and fraud prevention policies that E-merchants are implementing.

Example: www.merchant911.org.

•To reverse a chargeback, be prepared to demonstrate to the credit card company that you and your customers have entered into binding on-line contracts which, for example, prohibits cardholders from initiating a chargeback on an order after your business refund period has lapsed. Seek guidance from an attorney who specializes in E-commerce law who can counsel you on how to create legal and enforceable online contract.

•When selling services on-line, don't accept the credit card order until you have faxed a written sales contract to the cardholder, and the cardholder has sent it back to you with his or her signature. Require the cardholder to send a retainer or down payment with the signed sales contract.

Recommended: If you sell services on-line, contact an attorney to draft your service contracts for the service agreements you need.

Reason: Unlike purchasing of merchandise sold over the Internet, when buying *services* such as Web development…on-line card transaction services, etc., customers are typically willing to sign a printed document and return it without hesitation.

Key: This alternative is better than simply having a customer click "Accept" on an on-line contract because you have a live signature to authenticate the transaction.

Contrast: When selling products on-line, E-merchants will lose customers if they demand a signed written agreement for purchases.

Caution: On-line shopping cart transactions usually do not create a legal and enforceable contract.

Self-defense: Contact an experienced attorney to draft a legal and enforceable on-line contract protecting you from preventable E-commerce rip-offs.

***Cyber-Crime Fighter* source:**

Mark W. Ishman, Principal Founder and Managing Member of Triangle Law Center, PLLC, www.ishmanlaw.com, an E-commerce law firm dedicated to assisting E-merchants with on-line business legal issues. Mark is currently filing class action lawsuits on behalf of all. E-merchants in their fight to make tomorrow a better day to conduct business on-line. Mark has a Masters in Law in Information Technology and Privacy Law.

CHECK FRAUD UPDATE

High-Tech Check Fraud Prevention:

PAPER'S DAYS ARE NUMBERED

Automated Clearing House (ACH) is the standard banking technology used to digitize check transactions to cut the time for checks to clear and to reduce processing costs for financial institutions. Ultimately, some experts predict, ACH will render conventional paper checks obsolete. For financial institutions as well as retail stores and high-volume billers such as large retail chains and utility companies, now is the time to start learning about new technologies that could make this prediction a reality in coming years.

HOW IT WORKS

ACH has two primary applications…

•**Point-of-purchase check payments.** With a point-of-purchase (POP) transaction, paper checks—which still account for more than 60% of non-cash transactions—can be read by a scanner after they're received by the merchant. The scanner records the MICR information and can create an electronic image of the check.

Ultimately some experts predict, ACH will render conventional paper checks obsolete

The scanned data can be validated against a nationwide fraud prevention database to determine if the account is fraudulent, closed or insufficiently funded to cover the transaction.

If the check is accepted, a sales receipt is printed and the customer is asked for authorization. Once the customer signs the receipt, the sales clerk voids the check which is destroyed at a later time.

An electronic transaction is generated, and the funds are transferred via ACH from the customer's account and deposited into the merchant's business account.

Any declined POP transactions can be displayed on the cashier's monitor while the customer is still present and the cashier can ask for another form of payment.

•**High-volume bill-paying/lockbox operations.** Because of its superfast processing speed, the ACH process also works in high-volume bill payment systems, such as retail or wholesale lockboxes. There, merchants reduce fraud risk because bad checks are returned much more quickly and fraudsters therefore have less float time to take advantage of.

Major new advance: A technology called Accounts Receivable Conversion (ARC). In combination with ACH, new high-tech check imaging machines enable high-volume payees such as utility companies, telephone companies, department store chains, etc. to have consumer checks rapidly scanned and immediately converted to ACH payments.

Result: Payments clear within two days instead of the normal three to five days.

With ARC, the original check is destroyed…and most customers don't even know about the digitized transaction unless they carefully read their bank statements. Instead of a check debit and check number showing up on the statement, customers see only an ACH debit amount.

Caution: As effective as ARC may be

Continued on page 4

THE HUMAN ELEMENT

On-Line Fraud Prevention Best Practice: NO-TECH

The percentage of on-line merchants enhancing preventative measures against on-line fraud grew to 69% in 2003 from 65% the previous year.

Odd reality: While the amount of high-tech commerce continues to swell, one of the fastest-growing fraud prevention tactics is manual review of suspicious transactions.

Trend: The number of E-commerce merchants that manually review transactions to catch fraud spiked from 52% in 2002 to 65% in 2003.

NO-TECH VERSUS HIGH-TECH

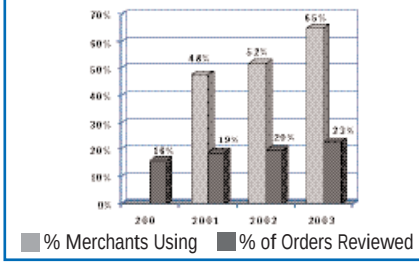
Address verification (AVS) is still the most widely used method for screening fraudulent on-line transactions. But manual review apparently still gives E-merchants a much greater sense of security than such higher-tech alternatives as CVN, Verified by Visa, MasterCard SecureCode or risk scoring.

...one of the fastest growing fraud prevention tactics is manual review of suspicious transactions

Added perspective: While the percentage of on-line orders being reviewed manually rose by just three points in 2003—to 23%—the *volume* of on-line sales jumped by 25% to 30%.

Result: E-commerce merchants must manually investigate many more orders now than ever, just to keep pace with the growth of E-commerce volume.

On-Line Merchants Are Manually Reviewing More On-Line Orders Before Accepting Them



WHAT TO EXPECT

Most forecasts of growth rates for on-line commerce indicate 25% to 35% annual growth over the next few years.

Implication: E-merchants that already manually review a large portion of their total orders will need to either divert more staff time to the order review process...hire more reviewers...allow more time to process and ship orders...or risk higher fraud losses by reducing the rate of suspicious order review.

IS IT WORTH IT?

E-merchants accept an average of two-thirds of the orders they decide to manually review. And many are accepting more than 90%.

Conclusion: Each company must measure the value of preempted frauds against the cost of achieving those reduced losses.

CHALLENGES TO GUIDE ANTI-FRAUD ACTION

Challenge #1: **Cost control.** Relying on manual intervention to prevent fraud usually means having to contact the consumer to validate on-line order information or to collect additional information.

This is a high-cost process, but one that few merchants see being able to dispense with anytime soon.

Key: Maximize the productivity and effectiveness of the manual review process so that as on-line order volume grows, hiring new people to control on-line credit card fraud is minimized.

Challenge #2: **Keeping fraud tools and strategies up-to-date on an ongoing basis,** as well as intelligently applying those tools to achieve the delicate equilibrium of reducing fraud, improving operational efficiency, boosting sales and minimizing the negative impact of fraud protection measures on customers.

***Cyber-Crime Fighter* source:**

5th Annual Online Fraud Report, Cybersource Corporation, a leading provider of electronic payment and risk management technology. The company is headquartered in Mountain View, CA and can be visited at www.cybersource.com.

For the full survey, go to http://www.cybersource.com/promo/2004fraud/index.html.

Continued from page 3

in catching NSF checks quickly enough to avoid fraud, the technology so far does not stop check counterfeiting and forgery. These crimes—by far the most common of all check frauds—must still be screened for by human eyes and intuitive brains.

The goods news: All of that is changing. *Examples:*

- **Forgery protection.** Technologies are being developed to enable high-speed signature verification from imaged checks at the teller's window to reduce the incidence of forgery before the fraudster leaves the branch.

...with ARC, most customers don't even know about the digitized transaction

- **Counterfeit reduction.** Because tech-savvy check counterfeiters know that they can often pass a bad check with just the stolen routing, account and MICR numbers on a legitimate-looking check (not necessarily a perfect reproduction of the victim's check), technology now being developed will be able to compare the check stock of the presented check with that of the legitimate account holder. Counterfeits are detected on the scene.
- **Check kiting prevention.** Because kiting often involves numerous financial institutions and takes advantage of the time delay of today's payment system, kiters operate on the premise of being able to gain access to deposited funds before they are collected from the institution on which they are drawn.

Clearing checks through near-instantaneous ACH conversion will dramatically shorten the physical transportation processing time, giving kiters a rude awakening, and greatly reducing check processing costs by eliminating the need for trucks, planes and trains to physically transport original checks.

Outlook: ACH, POP and ARC won't eliminate the need for human detection of counterfeit and forged checks for many years. However, it will give high-tech fraudsters new challenges to overcome the constant attempt to stay a step ahead of banks, merchants and their customers.

In the future, ACH will be able to eliminate the use of paper checks for clearing and settlement, forcing fraudsters to devise new ways to rip off banks, retailers and their customers. Already, check and payment fraud prevention experts

Continued on page 5

Continued from page 4

are anticipating the rise of fraud rings that will generate high volumes of bogus electronic payments for small amounts, with the intention of operating "below the system's radar" of fraud filtering.

In addition, identity theft will remain an invaluable tool for fraudsters in the increasingly electronic environment of check payments

Reason: Creating a bogus electronic payment account using someone else's personal identifying information will remain as easy as it is in today's paper checking account world.

The bottom line: The new high-speed clearing and technological advances for check fraud prevention will give financial institutions, retailers and consumers powerful tools in fighting check fraud. But the technology for making this happen must be implemented quickly to prevent the fast-moving check criminals from outsmarting this latest stage in the ongoing war between the legitimate financial services industry and the growing number of shrewd criminals who remain in hot pursuit of illegal gains.

***Cyber-Crime Fighter* sources:**

•Bill Robertson, Check Product Line Director, Wausau Financial Systems, www.wausaufs.com.

•Jodi Pratt, Senior Vice President, Carreker Corp., www.carreker.com. Jodi can be reached at jpratt@carreker.com.

•*A Guide to Electronic Check Conversion Services,* Wachovia Bank, www.wachovia.com /file/sell_electronic_check_conversion.pdf.

How the World's Toughest Security Machine Does Security

The Israeli military is installing a super-high-tech biometric identification system at a Gaza Strip checkpoint to speed the daily crossing of Palestinian workers who travel to menial jobs in Israel.

The system: Developed by On Track Innovations Ltd. (OTI) of Rosh Pina, Israel, the security system uses two biometric sensors to read the facial dimensions and hand geometry of Palestinian workers passing through the Erez checkpoint—the busiest on the Israeli-Gaza border.

Key: Workers will carry new smart cards that contain their encoded facial and hand biometrics. At the checkpoint, they will have their faces and hands scanned to make sure they match the data stored on the cards.

***Cyber-Crime Fighter* source:**

Ohad Bashan, director of global marketing, On Track Innovations., Ltd., www.oti.co.il, quoted in *washingtonpost.com*.

E-BANKING FRAUD

AUTHENTICATE BEFORE IT'S TOO LATE:

Fraud-Prevention Strategies for On-Line Banking

On-line banking is expanding rapidly, but unfortunately, electronic bank fraud is growing right along with it.

Old scams…new tools: With basic computer skills, fraudsters abuse the cyber-banking system by using stolen identities to open new accounts and by "taking over" established accounts to steal legitimate customers' money.

CONVENIENCE VERSUS CRIME CONTROL

Challenge: The financial services industry must strike a delicate balance between offering customers excellent service and convenience for opening and managing on-line accounts…and implementing safeguards that thwart cyber-banking fraudsters.

Success secrets: Earn on-line banking customers' cooperation and goodwill by educating them about the new electronic tools fraudsters use…and letting them know the reasons behind inconvenient on-line banking security procedures—such as asking for "atypical" types of personal information, like the city they were born in…the name of the high school they attended, etc.—and requiring frequent password changes.

LOW-TECH PROTECTION

Not all anti-fraud strategies cost bundles of money and take weeks of IT development time to design and implement. Some lower-tech, but highly effective solutions include…

•Requiring new accounts to be opened in a branch. It's quite a bit more difficult for a 25-year-old man to impersonate a 60-year-old woman if he's standing in front of a bank employee filling out his application.

Also key: Have prospective customers put their signature on their application—preferably in front of you or a trained customer service representative who can authenticate the signature. That way you have a signature on file with which to compare checks, loan payments, loan applications, etc.

•Limiting the application timeframe…on-line and on paper. If your organization does accept on-line banking applications completed on its Web site, tell prospective customers the application page will "expire" if too much time is taken to complete each field…and impose time limits on paper applications as well.

Result: Identity thieves won't be able to spend hours or weeks researching people's lives to find answers to questions that might go beyond usual personal identifiers like Social Security number, date of birth, address and mother's maiden name.

•Asking "in-wallet" and "out-of-wallet" questions. "In-wallet" questions—the information on a driver's license…credit card numbers, etc.—tells you that the person opening a new account or applying for credit actually exists.

"Out-of-wallet" questions come from a person's credit history. They're detailed, unique and often trip up fraudsters attempting to lie.

Sample questions: Which of the following lenders holds your first mortgage? How much is your monthly mortgage payment? With which lender do you currently have a home equity line of credit?

•Asking "out-of-credit" questions. Answers to these unique, personal questions are typically known only to an authentic applicant—though one or two might be verifiable by using non-financial records, such as county real estate records. *Examples:*

☐ How many bathrooms do you have in your house?

☐How many people currently live in

Continued on page 6

NEED-TO-KNOW HOT LINE

Signs of Success in Cooperative Cyber-Crime Law Enforcement

The 125-plus arrests and more than 70 indictments resulting from the first six months of Operation Cyber-Sweep indicate that law enforcement agencies may be coming up with effective ways to collaborate in busting cyber-criminals.

Key: The large number of arrests and indictments is at least in part due to the coordinated effort between the FBI, US Secret Service, Postal Inspectors, the FTC, Bureau of Immigration Customs Enforcement. Additional state, local and foreign law enforcement agencies also have been playing active roles in the operation.

Additional lesson: The Operation Cyber-Sweep team provided powerful new evidence of the fact that cyber-economic crimes are rapidly evolving into global offenses, requiring sophisticated multi-jurisdictional enforcement action.

Main targets of Operation Cyber-Sweep: On-line use of counterfeit credit cards…cyber-securities fraud…hacking of all kinds…cyber-extortion…identity theft.

Operation Cyber-Sweep is a substantially enhanced follow-up to Operation E-Con, announced by Attorney General Ashcroft in May 2003.

The new, ongoing operation was launched in response to a jump in the reporting of Internet-related complaints to federal agencies. The Internet Fraud Complaint Center (IFCC)—www.ifccfbi.gov—referred 58,392 Internet-related fraud complaints to law enforcement in the first nine months of 2003.

Contrast: In the full year 2002, IFCC referred about 48,000 Internet-related fraud complaints to law enforcement.

For a list of specific cyber-crime cases resulting from Operation Cyber-Sweep, visit: http://www.usdoj.gov/opa/pr/2003/November/03_crm_639.htm.

Don't Let Precious IT Security Dollars Go to Waste

Despite encouraging data about spending on IT security, one of the country's top infosec experts sees serious flaws in the way those security dollars are being allocated.

According to the Meta Group's latest survey of corporate spending on IT spending, companies spent 8.2% of their total IT budgets on security—up from 7.6% in 2002 and more than double the 3.2% level of 2001.

Not surprisingly, corporate security programs have been focused primarily on employee education, business continuity and disaster recovery.

Problem: Not all of the news is good, according to Alan Paller, Director of Research at the SANS Institute. While encouraged by the increased dollars being budgeted for IT security, Alan says that the investment isn't paying off in improved infosec defenses. He reports that "Apparently a large portion of the increased funding is being spent on consultants who write reports required by regulation. Those consultant studies are consuming so much money that budgets for vulnerability elimination and perimeter protection and identity management is actually being reduced to pay for the studies."

Solution: Pressure on the US Congress. Alan invites companies that find more than half their IT budgets are being consumed by report-writing for regulators to notify SANS.

Reason: "Congress doesn't want to exacerbate the problem" Alan says, "but if the only people they hear from are lobbyists from the consulting and vendor community, then they have no way of finding out what's happening in the real world."

***Cyber-Crime Fighter* sources:**

- META Group's 2004 Worldwide IT Benchmark Report, www.metagroup.com.
- Alan Paller, Director of Research, SANS Institute, www.sans.org.

Continued from page 5

your house?

☐ How many siblings do you have?

☐ In what city did you attend high school?

☐ What kind of car do you currently drive?

☐ What was the name of the first family pet you can remember having as a child?

- **Verifying application data beyond the obvious—**Social Security number, phone number, birth certificate records and driver's license information.

Example: The customer's snail-mail account supplied in the original on-line or mailed-in application should match the US Postal Service records for the person, as well as the address at which statements are to be received.

With basic computer skills fraudsters abuse the cyber-banking system by using stolen identities

Reason: Often, fraudsters will use a real person's demographic information to apply for an account with on-line banking features and, within a day or two of submitting the application, will call to request a change of address. Mailing verification to the original address on the application ensures that a legitimate person completed the original application—or alerts the on-line banking customer to an act of identity theft in the making.

- **Partnering with third-party suppliers of application pattern-recognition services to spot over-used "personas,"** false addresses, fraudulent uses of deceased people's personal information, behavior outside of the norm—why might an 80-year-old suddenly open a new account with on-line management features?—etc.

Top third-party suppliers: The three credit bureaus, Equifax, Experian, Trans Union, as well as ChexSystems, eFunds.

MAINTAINING ACCOUNT SECURITY

To prevent "account takeover" attempts after a legitimate customer has opened a new account, educate customers on how to minimize the potential for Trojan infections. These are perpetrated by hackers planting sophisticated keystroke logging and other eavesdropping software on victims' PCs. Most on-line users won't detect Trojan horses once their systems are infected. User education should focus on safer and smarter Internet browsing and file

Continued from page 6

downloading practices—and what to do if a Trojan is found.

Essential: Require customers to self-select a user ID that identifies them when they log-in to your financial services Web site. This is not a PIN number. It is for bank employees to verify who they're dealing with if they need to help a customer with an account. Since it's self-selected, it helps guard against fraudulent entry to the account.

For added security: Have the customer also select an Internet password known to no one but him/herself. Enable this password to contain up to 20 characters—the more the better—and store all passwords in an encrypted format at your company so that they're not easily accessed by technologically gifted—but dishonest—employees.

Helpful: When advising new customers of the need for—and the process of—selecting a password, inform them that this security strategy keeps even your customer service reps in the dark as far as their private password is concerned. Telling them now may eliminate the frustration they feel in the future when they lose or forget their password and it takes time to restore their on-line banking access.

POST SET-UP STEPS

Two essential authentication steps after a customer has applied for on-line banking services …

•**Mail out a "Welcome to On-line Banking" letter.** This letter, sent to the statement mailing address, should instruct the recipient to call or E-mail your institution immediately if he or she did not set up the new account.

•**Track customer behavior for at least 30 days.** Watch for suspicious activity—large withdrawals/transfers, large deposits, unusually frequent account access, account address changes, etc. If you notice suspicious behavior, take action to block account access and contact the customer with your concerns.

***Cyber-Crime Fighter* sources:**

•*Fraud Prevention Strategies for Internet Banking.* Excerpts adapted with permission. The full text of the paper is available at the BITS web site at www.bitsinfo.org/wp.html.

•Peter Vogt, President, Information Systems Security Association (ISSA) Connecticut Chapter, www.issa-ct.org, president@issa-ct.org. Peter is an expert in enterprise security, data privacy and identity fraud.

•Allan Trosclair, a fraud-loss control consultant, former FBI Special Agent and former vice president, fraud control for Visa USA. Allan can be reached at trosclair@verizon.net.

Inside Scoop

From Cyber-Crime Fighter's files from the field…

Nigerian E-mail Scam Leads to Murder

Michael Lekara Wayid, the Nigerian consul to the Czech Republic, was fatally shot earlier this year by a 72-year-old man who reportedly was victimized by one of the all-too-frequent Nigerian E-mail scam operations.

Details: Having lost his life savings to the scammers, the victim called the Nigerian Embassy in Prague to complain and request assistance. Having evidently failed to receive the response he had expected, he visited the Embassy and fired a gun at Mr. Wayid, killing him and wounding a clerk. He was arrested at the scene.

***Cyber-Crime Fighter* source:**

ZDNetUK, http;//www.zknet.co.uk/.

Keeping Infosec Staff Up to Snuff

Effective cyber-security technique: Give information security staff verbal pop quizzes to make sure they are up-to-date with latest security threats and the company's latest incident response tactics.

Example: Create hypothetical cyber-security incident scenarios and ask security personnel for exact steps they would take to respond. Errors and misjudgments can then be corrected before a real breach occurs.

Also helpful: Make sure every staff member spends a certain amount of work time in scheduled infosec awareness sessions covering the latest cyber-incident trends and new security technologies.

***Cyber-Crime Fighter* source:**

Walt Foultz, Director of IT security for Farmers Insurance Group, quoted in CSOonline, http://www.csoonline.com/read/050103/bad.html.

For Better, Safer Passwords

Did you know that you may only need three passwords to maintain maximum information security in any computer activity you engage in?

How: First, sort the umpteen passwords you use into three groups, with one password for each…

•**Low security**. These can include your Yahoo E-mail password, Instant Messenger password and the password for the countless Web sites that make you register with a userID.

Choose a single password for all of these low-security Web destinations. It can be just letters, just numbers or a mixture of both.

Critical: Only you should be able to decipher the meaning of the password.

•**High security.** These are your bank and credit card PIN numbers. A PIN is usually used at public machines, like an ATM or a point-of-sale debit card terminal. PIN numbers normally are four or six digits long.

Best: A four-digit PIN, because you can then use the same PIN for your bank card, on-line banking account, etc.

•**Complex.** If you have personal information that you don't want anyone to access, this password is the most secure. It also is effective for corporate network security. It must be created with care and be "un-guessable." Think not in terms of letters and numbers, but in terms of passphrases.

Example: SeattleSeahawksSingSad

Coming Soon in *Cyber-Crime Fighter*

•Using biometrics to foil computer crime

•Making computer usage policies work throughout the organization

•Computer forensics: A case history

•Curbing internal cyber-crime

•New E-mail legal standards

SongS4M E. As a password it would read, SSSSS4M.

But a secure password should also contain upper and lower case letters, so you can adjust the password to read SSSSS4m. Lastly, because the toughest passwords also include a special character, you could add a "$" sign and end up with a secure and easily remember: $SSSSS4m.

Next: Add to those three groups your master password. This is the one to access all your other passwords. Once you create it, never write it down anywhere. For peace of mind, store all of your passwords in an encrypted "safe."

Recommended: Password Safe (http://prdownloads.sourceforge.net/passwordsafe/pwsafe-1.9.2b-bin.zip?download), a free application that is easy to use and extremely secure. It uses the Blowfish cryptography algorithm to protect all of your passwords with one "safe combination."

***Cyber-Crime Fighter* source:**

Vanish.org, www.vanish,.org, a Web site providing practical information on password creation and protection, anti-spam tactics, Internet fraud prevention and more.

Spyware Busting Update

The incidence of intrusion via eavesdropping spyware by employees, ex-employees, competitors and others is rising, according to infosec experts. Key-logging applications such as Eblaster and Spyware are increasingly popular for electronic eavesdropping. Unfortunately, while it is illegal to install such software on a PC you don't own, today's applications are typically installed, unknowingly, by the user.

Naturally, a counter-industry of anti-spyware software exists and it is reportedly doing quite well

Problem: No single anti-spyware application is completely effective on a single PC. Until someone comes up with an anti-virus-like application that comprehensively screens for implanted key-logging and other spyware, many concerned computer users will continue to install multiple protective products.The consensus from an informal poll on an infosec forum showed that the most popular choices are Spybot, SpywareGuard, SpywareBlaster and Ad-aware.

Caution: The experts have differing opinions about the effectiveness of each of these leading products, so before installing, check with colleagues and infosec specialists you have confidence in…and who have direct experience with the products.

***Cyber-Crime Fighter* sources:**

- Internet security forums.
- http://spπ ycop.com/.
- Prominent information security professionals.

InfoSec Awareness Training Trap to Avoid

The good news is that more and more companies are realizing that their employees are often the weakest link in the information security chain. Many are taking action by implementing security training awareness programs for the entire workforce.

The bad news: Too many companies use a "fire hose" approach to security awareness, deluging employees with a full year's worth of information security content in a one-day training session.

Result: Because of the information overload, very little is actually retained and employees are so relieved when they complete the session that the last thing they want to be aware of is information security.

Solution: A year-round program that concentrates on a small number of infosec topics each quarter.

Consider covering authorized/appropriate usage and virus protection in one quarter and move in quarterly sequence to such topics as worms,Trojan horses, network security, safe surfing, etc.

***Cyber-Crime Fighter* source:**

Bernie Cowens, CISSP, Vice President of Security Services, Rainbow Technologies, software security and cryptographic technology providers, www.rainbowtechnologies.com, writing in *ISSA Journal,* www.issa.org

On the Calendar

The 13th annual RSA Conference, one of the biggest gatherings of infosec professionals, corporate executives, policy makers and investigators, will be held February 23 through 27, 2004. Sample educational tracks…

- **Hacker & Threats**—insights into hacking, network forensics and countermeasures.
- **Privacy, Law and Policy**—topics of interest to lawmakers, privacy activists, policymakers, attorneys and public-interest groups.
- **Identity and Access Management**—focusing on access control, authentication, identification technologies and protocols and the worsening threat of identity theft.

More information: http://2004.rsaconference.com/.