

Home

## [A Little Fraud Among Friends](#)

Archive

Links

### **International Israeli Internet Spying & Fraud**

Contact Us

April 4, 2006

Webmaster

by Michael Bagley, Financial Editor

For the past five years, there have been growing fears that somehow, outsiders have been able to penetrate into the confidential computer files of government agencies, business entities such as banks and defense contractors and individuals.

Some of this appeared to be an attempt to obtain highly classified information that could be of use to others and in other instances, attempts to get into the personal, and corporate, bank accounts of individuals and corporations.

This is a brief study of some of the salient aspects of this problem of computer theft and espionage and we will start with the discovery of massive computer penetration in Israel. We will then consider further penetrations of American business and intelligence computer systems by agents of a foreign government as opposed to confidence men and then conclude with the use of the same methods to commit frauds on the gullible in the United States and elsewhere.

Some of the first public notice of this problem surfaced first in Israel in 2004 when Israeli law enforcement cyber crime experts discovered that what is known as a Trojan Horse (illicit spyware planted on an unsuspecting computer) had been inserted into about 60 major Israeli businesses. Israeli law enforcement subsequently indicted various members of three of Israel's largest private investigative agencies on charges of criminal fraud. These spyware plants were in various commercial areas such as : Israeli military contracting, telephone systems, cable television, finance, automobile and cigarette importing, journalism and high technology. These intrusive spyware plants were nearly identical with ones developed by the American NSA and widely used inside the United States to glean political, economic and counter-intelligence information from a huge number of American businesses and agencies. Israeli investigators believed that there was illicit cooperation between the American agency and a counterpart in Israel.

These

Trojan horses that penetrated the Israeli computers came packaged inside a compact disc or were sent as an e-mail message that appeared to be from an institution or a person that the victims thought they knew very well. Once the program was installed, it functioned every time the victim's computer system was in use, logging keystrokes or collecting sensitive documents and passwords before transmitting the information elsewhere.

This clandestine theft of valuable commercial, military and political secrets is certainly not limited to Israel and many important agencies and individuals have become increasingly concerned about what is called "phishing" in which both con men and foreign (and domestic) intelligence agencies can locate, capture and use valuable personal, political and financial information. In September of 2005, the Anti-Phishing Working Group, an ad hoc group of corporate and law enforcement groups that track identity theft and other online crimes, said it had received more than 13,000 unique reports of phishing schemes in that month alone, up from nearly 7,000 in the month of October, 2004..

In late 2005, a new form of phishing, called "spear-phishing" emerged.

.So-called spear-phishing is a highly concentrated and far more effective version of phishing. That's because those behind the schemes bait their hooks for specific victims instead of casting a broad, ill-defined net across cyberspace hoping to catch throngs of unknown victims.

Spear-phishing, say security specialists, is much harder to detect than phishing. Bogus e-mail messages and Web sites not only look like near perfect replicas of communiqués from e-commerce companies like eBay or its PayPal service, banks or even a victim's employer, but

are also targeted at people known to have an established relationship with the sender being mimicked. American banks such as Chase and Bank of America are among those whose names are faked and also the online auction house of Ebay and the international money transfer firm of PayPal receive considerable attention from the international conmen and credit thieves. These thieves are not necessarily gangs operating for financial gain but also include theft of trade secrets, private corporate banking and highly sensitive military and political information.

While some of these phishers are merely out to make money, others are interested in securing military secrets and political activities, all at the highest and what is hopefully considered as the most secure.

As a case in point, in June of 2005, the National Infrastructure Security Coordination Centre, a British government agency that monitors national UK computer security, took the step of publicly warning about a spear-phishing campaign of "targeted Trojan e-mail attacks" aimed at industrial and government computer networks. The warning noted that the e-mail messages appeared to come from a trusted sender, that antivirus software and firewalls was completely incapable of protecting recipients, and that, in fact, there was no way to completely protect any computer connected to the Internet from the Trojan attacks once recipients opened and downloaded a faked e-mail message containing a virus.

The report noted that: "Files used by the attackers are often publicly available on the Web or have been sent to distribution lists," the warning said. "The attackers are able to receive, trojanise and resend a document within 120 minutes of its release, indicating a high level of sophistication."

In December of 2005, a more traditional phishing scam infected about 30,000 individual computers worldwide, according to CipherTrust, a computer security firm. Consisting of what CipherTrust said was about 50 million e-mail messages that a German hacker deployed simultaneously, the communiqués purported to come from the Federal Bureau of Investigation, the Central Intelligence Agency and a German intelligence agency and tried to convince recipients to provide personal information and open a file containing a virus. The F.B.I. issued a warning about the scheme and a spokeswoman said that thousands of people swamped the agency with phone calls inquiring about it. Public awareness and FBI actions sharply reduced and finally obliterated this specific form of fraud but no information has been released to the public by the FBI concerning the identity or motives of many of the hackers. No bank or financial institution ever contacts their depositors and customers by email with warnings about misuse of their credit cards or errors in their personal accounts. The phishers have advanced technologically to the point where actual company logos can be snatched from Web sites to build customized databases of corporate logos. Any email message purporting to come from any bank or financial institution, most especially one that has the proper company logo and format but contains grammatical errors should ever be responded to.

Some computer security specialists suggest at least one basic approach that might allow e-mail recipients to learn right away that a communiqué appearing to come from a company like Amazon.com actually originated somewhere in the Ukraine, Romania, Bulgaria, Poland, Russia or any of the other places that law enforcement officials say are hot spots for phishing scams. According to CipherTrust, a spear-phisher can rent a server for about \$300 month after paying a \$100 setup fee; install spam-sending software on the server for about \$1,200 a month; and get spam-sending proxies, a database of e-mail addresses, and other necessary add-ons for another \$1,900 a month. How much phishers make depends on how many victims they hook, but the relatively small expense means the work can be lucrative. According to a research report issued in June by Gartner Inc., a consulting firm, about 2.4 million Americans reported losing about \$929 million to phishing schemes during the previous year.

In 2005, it has been estimated by the FBI and private cyper-protection agencies that about 73 million American adults who use the Internet believed that they received an average of more than 50 phishing e-mails during the prior 12 months. And that, of course, is just what Internet users actually know might be happening.

Phishers main goal is to obtain a victim's checking-account number and, in addition, credit card and A.T.M. card numbers, which they can copy onto bogus cards they have manufactured for the purpose of extracting money and goods from a victim's account.

It should be noted that many American banks have serious security gaps in the software used to analyze magnetic stripe coding on the back of A.T.M. cards, and these gaps have permitted card hijackers to use bogus copies. American regulators, concerned about online vulnerabilities at the country's banks, have sharply tightened security requirements at financial institutions.

Although Internet Provider (IP) numbers lead to Italy, the Netherlands, the Ukraine, Romania, Bulgaria, Poland, and Russia, a secret investigation by NSA and other American domestic and foreign intelligence agencies has disclosed that almost all of the scams originate inside Israel and that while the Israeli authorities are aware of this, the fact that information considered “vital to the interests of the State of Israel” is part of the intercepts, no action has been taken against operations that are not directed against Israeli agencies or individuals. Further, one of the caveats to the continued functioning of these enormously profitable computer frauds is that any monies gleaned from them must be deposited in Israeli, and not foreign, banks.

Israeli intelligence, having formed a cooperative association with Israeli internet swindlers, has, according to an NSA report, not hesitated to spy on their American counterparts.

Among the Israeli corporations on the receiving end of stolen information were two telecommunications affiliates of Bezeq, the country's largest telephone company. The Israeli government held a controlling interest in Bezeq until it sold most of its stake to private investors, including Los Angeles media mogul Haim Saban, shortly before the Trojan horse scandal became public. A lawyer representing Bezeq and the two affiliates, YES and Pele-Phone, declined to comment on the investigation; Mr. Wisomsky said that Bezeq itself appeared to have been a victim, not a recipient, of stolen information.

Israeli intelligence also is able to oversee almost all telephonic contacts, to include internet usage, in the United States.

This is accomplished by obtaining and analyzing data that is generated every time someone in the U.S. makes a telephone call.

Here is how the system works. Most directory assistance calls, and *virtually all* call records and billing inside the U.S. are done for the telephone companies by *Amdocs* Ltd., an Israeli-based private telecommunications company.

*Amdocs* has contracts with the 25 biggest telephone companies in America, and even more worldwide. The White House and other secure government phone lines are protected, but it is virtually impossible for any American to make a call on any American phone without generating an *Amdocs* record of it.

In recent years, the FBI and other government agencies have investigated *Amdocs* more than once. The firm has repeatedly and adamantly denied any security breaches or wrongdoing. In 1999, the super secret National Security Agency, headquartered in Ft. George Meade in northern Maryland, issued what is called a Top Secret Sensitive Compartmentalized Information report, TS/SCI, warning that records of calls in the United States were getting into foreign hands – in Israel, in particular.

Investigators do not believe such calls are being listened to, but the data about who is calling whom and when is extremely valuable in itself. An internal *Amdocs* memo to senior company executives suggests just how *Amdocs* generated call records could be used. “*Widespread data mining techniques and algorithms...combining both the properties of the customer (e.g., credit rating) and properties of the specific ‘behavior....’*” Specific behavior, such as who the targeted customers are calling is also noted.

The *Amdocs* memo says the system should be publicly advertised as “*helping to prevent telephone fraud.*” However, U.S. counterintelligence analysts say it could, and unquestionably was, also be used to spy via the records of the American telephone system. The N.S.A has held numerous classified conferences to warn the F.B.I. and C.I.A. how *Amdocs* records could be used.

At one classified NSA briefing, a diagram by the Argonne National Laboratory was used to show that if phone records are not completely secure, major security breaches are more than possible.

Another NSA briefing document said, “*It has become increasingly apparent that systems and networks are vulnerable...Such crimes always involve unauthorized persons, or persons who exceed their authorization...citing on exploitable vulnerabilities.*”

Those vulnerabilities are growing, because according to another briefing, the U.S. relies too much on foreign companies like *Amdocs* for high-tech equipment and software. “*Many factors have led to increased dependence on code developed overseas.... We buy rather than train or develop solutions.*”

U.S. intelligence does not *officially* believe the Israeli government is involved in a misuse of information, and *Amdocs* insists that its data is secure. What U.S. government officials are worried about, however, is the possibility that *Amdocs* data could get into the wrong hands, particularly organized crime. And that would not be the first time that such a thing has happened.

In a 1997 drug trafficking case in Los Angeles, telephone information, specifically of the type that *Amdocs* collects, was used to "*completely compromise the communications of the FBI, the Secret Service, the DEA and the LAPD.*"

There has been considerable but very quiet concern about the 60 Israelis who were detained in the anti-terror investigation, and the suspicion that some investigators have that they may have picked up information on the 9/11 attacks ahead of time and not passed it on.

There exists a classified Justice Department report stating that the *Mossad*, the Israeli intelligence agency, did indeed send representatives to the U.S. to warn, just before 9/11, that a major terrorist attack was imminent. How does that leave room for the lack of a warning?

What investigators have stated is that that warning from the *Mossad* was nonspecific and extremely vague and general, and they believe that it may have had something to do with the Israeli desire to protect what are called "sources and methods" in the intelligence community while at the same time attempting to convince American authorities that they were being cooperative and friendly. There is very substantive and documented evidence that those sources and methods were, and still are, taking place in the United States.

The question arose in the Select Intelligence Committee on Capitol Hill, chaired by former CIA agent, Porter Goss. Concern was expressed concerning this *Mossad* spying issue but nothing came of this and the matter was very quickly, and quietly, shelved

An official listing of known *Mossad* agents and a much larger one listing *Mossad* informants in the United States is perhaps the best indicator of the degree and extent that this official Israeli organ has penetrated American security, business and military organizations. Its publication would certainly create terrible havoc and would very adversely impact on American/Israeli diplomatic and military relations.

Reports indicate that such established agencies as the Anti Defamation League, several identified national newspapers and one major television network also harbor and assist a significant number of active *Mossad* agents engaged in espionage activities.

The concern about telephone security extends to another company, founded in Israel, that provides the technology used by the U.S. government for electronic eavesdropping. The company is *Comverse Infosys*, a subsidiary of an Israeli-run private telecommunications firm, with offices throughout the U.S. It provides wiretapping equipment for law enforcement. Investigative reports also indicate that these offices have been and are being used as bases for intelligence operations directed against the United States via the *Mossad* agents working in this country.

Here is the method that foreign wiretapping works in the U.S.

Every time a call is made in America, it passes through the nation's elaborate network of switchers and routers run by the phone companies. Custom computers and software, made by companies like *Comverse*, are tied into that network to intercept, record and store the wiretapped calls, and at the same time transmit them to investigators.

The manufacturers have continuing access to the computers so they can service them and keep them free of technical errors. This process was authorized by the 1994 *Communications Assistance for Law Enforcement Act*, or CALEA. Senior government officials have reluctantly acknowledged that while CALEA made officially authorized, and unauthorized, wiretapping much easier for Federal authorities, it has led to a system that is seriously vulnerable to compromise, and may have undermined the whole wiretapping system.

Attorney General John Ashcroft and FBI Director Robert Mueller were both warned on October 18, 2001 in a hand-delivered letter from 15 local, state and federal law enforcement officials, who complained that "*law enforcement's current electronic surveillance capabilities are less effective today than they were at the time CALEA was enacted.*"

Congress insists the equipment it permits to be installed is secure. But the complaint about this system is that the wiretap computer programs made by *Comverse* have, in effect, a back door through which wiretaps themselves can be intercepted by unauthorized parties.

In this case, the unauthorized parties is the Israeli *Mossad* and through them, the government and commercial interests of Israel itself.

Adding to the suspicions is the fact that in Israel, *Comverse* works closely with the Israeli government, and under special programs and gets reimbursed for up to 50 percent of its research and development costs by the Israeli Ministry of Industry and Trade. But investigators within the DEA, INS and FBI have all privately stated that to pursue or even suggest Israeli spying through *Comverse* is considered career suicide because of the enormous political and political power wielded by the Israeli lobby, the extremely pro-Israeli American television and print media and many Jewish financial organizations in the United States.

And sources say that while various F.B.I. inquiries into *Comverse* have been conducted over the years, they have been halted before the actual equipment has ever been thoroughly tested for leaks. A 1999 F.C.C. document indicates several government agencies expressed deep concerns that too many unauthorized non-law enforcement personnel can access the wiretap system. The FBI's own small office in Chantilly, Virginia that actually oversees the CALEA wiretapping program, is among the most agitated about the Israeli ongoing threat.

It is the FBI's office in Quantico, Virginia, that has jurisdiction over awarding contracts and buying intercept equipment. And for years, they have awarded the majority of the business to *Comverse*. A handful of former U.S. law enforcement officials involved in awarding *Comverse* lucrative U.S. government contracts over the years now work for the Israeli-based company.

Numerous sources say some of those individuals were asked to leave government service under what knowledgeable sources call "*troublesome circumstances*" that still remain under administrative review within the Justice Department.

And what troubles investigators the most, particularly in New York City, in the counter terrorism investigation of the World Trade Center attack, is that in a number of cases, suspects they had sought to wiretap and survey immediately changed their telecommunications processes. This began as soon as those supposedly secret wiretaps went into place

There are growing and very serious concerns in a very significant number of top-level American intelligence and counterintelligence. Many of these agencies have begun compiling evidence, and instigating a very highly classified investigation, into the very strong probability that the Israeli government is directly involved in this matter and has been from the outset.

Speaking confidentially, top U.S. intelligence agencies indicate that "*the last thing needed is another Pollard scandal.*"

Following the 9/11 attacks, Federal officials have arrested or detained nearly 200 Israeli citizens suspected of belonging to an "*organized intelligence-gathering operation.*" The Bush administration has deported most of those arrested after Sept. 11, although some are in custody under the new anti-terrorism law. Some of these detainees are being investigated for their possible penetration of known Arab terrorist groups located in the United States, Canada and Europe and through this, having gained specific knowledge of the time and location of the September 11 attacks.

It has been established that an Israeli firm generated billing data that could be used for intelligence purpose, and a recent Justice Department report describes concerns that the federal government's own wiretapping system may be vulnerable.

In Los Angeles, in 1997, a major local, state and federal drug investigation suddenly collapsed. The suspects: Israeli organized crime organizations, composed mostly of Russian Jews, with ongoing operations in New York, Miami, Las Vegas, Canada, Israel and Egypt.

The allegations: cocaine and ecstasy trafficking, and sophisticated white-collar credit card and computer fraud. . A DEA report under date of December 18 stated that there existed serious security breaches in DEA telecommunications by unauthorized "foreign nationals" -- and cites an Israeli-owned firm with which the DEA contracted for wiretap equipment .

The problem: according to classified law enforcement documents, is that the Israeli-based gangsters had the Federal and State law enforcement beepers, cell phones, even home phones under constant surveillance. Some identified Israeli gangsters who did get caught, readily admitted to having hundreds of confidential law enforcement telephone and beeper numbers and had been using them to avoid arrest.

An official LAPD intelligence report states:

*"This compromised law enforcement communications between LAPD detectives and other assigned law enforcement officers working various aspects of the case. The Israeli-based criminal organization discovered communications between organized crime intelligence division detectives, the FBI and the Secret Service."*

Shock spread from the DEA to the FBI in Washington, and then the CIA. An investigation of the problem, according to law enforcement documents, concluded, *"The (criminal) organization has apparent extensive access to database systems used to identify pertinent personal and biographical information."*

When investigators tried to find out where the information might have come from, they looked at *Amdocs*, a publicly traded firm based in Israel. *Amdocs* generates billing data for virtually every call in America, and they do credit checks. The company denies any leaks, but investigators still fear that the firm's data is getting into the wrong hands.

When investigators checked their own wiretapping system for leaks, they grew concerned about potential vulnerabilities in the computers that intercept, record and store the wiretapped calls. A main contractor is *Comverse Infosys*, which works closely with the Israeli government, and under a special grant program, is reimbursed for up to 50 percent of its research and development costs by Israel's Ministry of Industry and Trade.

Asked about another sprawling investigation and the detention of 60 Israelis since Sept. 11, the Bush administration treated the questions with frightened circumspection. The reason for this is also contained in the body of several U.S. investigative and highly classified reports. The extremely competent Israeli Foreign Intelligence branch, the MOSSAD, had penetrated the groups of terrorists who planned, and eventually executed, the hijacked aircraft attack on the World Trade Center, the Pentagon and the White House. After some debate in the highest official circles in Tel Aviv, the Israeli government decided to pass the very concrete and specific information about the September 11<sup>th</sup> attack to competent authority in the United States. This was done on three specific occasions, the Department of State, the CIA and the NSC all having been given MOSSAD reports. The nature and specific targets of the attacks were specified as were two different probable dates of attack. That the Bush Administration was informed of this planned attack by a putative ally and in specific detail and did nothing to attempt to circumvent it, came as a great surprise to Israeli officials. When it became obvious to them that their specific and timely warnings were obviously ignored, it then put Israel politicians in the position of having information which, if released to the American public, would cause terminal political damage, they decided, according to intercepted internet communication, that silence would guarantee future cooperation by the compromised Bush administration in any questionable Israeli political or military adventures in the Middle East.

### **Examples of typical email frauds**

#### ***Example No 1***

From : <information\_vital@virgilio.it>

Reply-To : <information\_vital@virgilio.it>

Sent : Tuesday, May 2, 2006 7:33 AM

Subject : Ticket No: 007802199001

Ticket No: 007802199001

RE: WINNING FINAL NOTIFICATION

LOTTO NL

INTERNATIONAL PRIZE AWARD DEPT.

Sir/Madam,

CONGRATULATIONS!!!

We happily announce to you the draw (#360) of the LOTTO NL INTERNATIONAL LOTTERY PROGRAMM, held on monday 1st of march 2006. It is yet to be unclaimed and you are getting the final NOTIFICATION as regards this. Your e-mail address attached to ticket number: 363775668993 7659 with Serial number 4571/06 drew the lucky numbers: 4-8-16-32-42-52 (bonus no.50), which subsequently won you the lottery in the 3rd category i.e match 5 plus bonus.

You have therefore been approved to claim a total sum of 2.450,000 (Two million four hundred and fifty thousand pounds sterling) in cash credited to file KTU/7034818304/06. This is from a total cash prize of 10,000,000 shared amongst the (5) lucky winners in this category i.e. Match 5 plus bonus. All participants for the online version were selected randomly from World Wide Web sites through computer draw system and extracted from over 100,000 unions, associations, and corporate bodies that are listed online. This promotion takes place weekly. Please note that your lucky winning number falls within our European booklet representative office in Europe as indicated in your play coupon. In view of this, your 2.450,000 (Two million four hundred and fifty thousand pounds sterling) will be released to you by any of oupayment offices in Europe.

Our European agent will immediately commence the process to facilitate the release of your funds as soon as you contact her. For security reasons, you are advised to keep your winning information confidential till your claim is processed and your money remitted to you in whatever manner you deem fit to claim your prize.

This is part of our precautionary measure to avoid double claiming and unwarranted abuse of this program.

Please be warned. To file for your claim, please contact our fiduciary agent:

Mr. Wim Molly

Tel: +31-616-557-921

Fax: ++31-847-136-657

Email:

dgclaimoffice1@netscape.net

1. FULL NAMES: \_\_\_\_\_

2. NATIONALITY: \_\_\_\_\_

3. AGE: \_\_\_\_\_

4. SEX: \_\_\_\_\_

5. MARITAL STATUS: \_\_\_\_\_

6. CONTACT ADDRESS: \_\_\_\_\_

7. TELEPHONE NUMBER: \_\_\_\_\_

8. OCCUPATION: \_\_\_\_\_

9. BRIEF DESCRIPTION OF COMPANY/INDIVIDUAL: \_\_\_\_\_

10. WINNING E-MAIL ADDRESS: \_\_\_\_\_

11. WINNING NUMBER: \_\_\_\_\_

12. TOTAL AMOUNT WON: \_\_\_\_\_

Endeavour to email/fax him your full names, winning numbers, email address, telephone and fax

numbers immediately.

Congratulations from me and members of staff of LOTTO NL LOTTERY.

Yours faithfully,

Mary Evens

Online coordinator for

LOTTO NL LOTTERY

Sweepstakes International Program.

**EXAMPLE No. 2**

From: Ernest Kemp [gvva@boskma.nl](mailto:gvva@boskma.nl)  
To: [brianharring@yahoo.com](mailto:brianharring@yahoo.com)  
Subject: practical  
Sent: Friday, April 28, 2006 10:11 PM

News was released.

Cyberhand Technologies International Starts Construction on Sound Activated Anti-Personnel

Fighting Robot Prototype. Go to yahoo financial and read it now...

Cyberhand Technologies International, Inc

CYHD,

Michael Burke, CEO of Cyberhand Technologies said, "Because of the potential collateral damage caused by some of today's weapons and missiles in enemy urban environments, we believe that our products will reduce the chances of injuring or killing innocent people in surrounding areas in which we strike."

About Cyberhand Technologies International Inc.

Cyberhand Technologies International Inc. focuses on Aerospace Weapons Systems that provide the world's fastest controllers and most accurate target acquisition, generating the best field results, as well as innovative wireless ergonomic products for private and military purposes.

Do your research now and start watching CYHD like a hawk.

Information within this report contains forward looking statements within the meaning of Section 27a of the Securities Act of 1933 and Section 21b of the SEC Act of 1934. Statements that involve discussions with projections of future events are not statements of historical fact and may be forward looking statements. Don't rely on them to make a decision. The Company is not a reporting company registered under the Exchange Act of 1934. We have received two million free trading shares and twenty five thousand dollars cash from a third party not an officer, director or affiliate shareholder. We intend to sell our shares now which could cause the shares to go down, resulting in losses for you.. This company has an accumulated deficit, nominal cash and no revenues in its most recent quarter with the float current increasing. The company may need financing to continue as a going concern. A failure to finance could cause the company to go out of business. Read the Company's Annual Report and Information Statement before you invest. This report shall not be construed as any kind of investment advise or solicitation. You

can lose all your money by investing in this stock.