

# Security Trends Report

05/08

## Criminals phish for CEOs via fake subpoenas

If you're going to cast your line, aim for the leviathan

By Robert McMillan

April 15, 2008 (IDG News Service) Panos Anastassiadis didn't click on the fake subpoena that popped into his in-box on Monday morning, but he runs a computer security company. Others were not so lucky.

In fact, security researchers said that thousands have fallen victim to an e-mail scam in which senior managers such as Anastassiadis are told that they have been sued in federal court and must click on a Web link to download court documents. Victims of the crime are taken to a phony Web site where they are told they need to install browser plug-in software to view the documents. That software gives the criminals access to the victim's computer.

This type of targeted e-mail attack, called "spear phishing," is a variation on the more common "phishing" attack. Both attacks use fake e-mail messages to try to lure victims to malicious Web sites, but with spear phishing, the attackers try to make their messages more believable by including information tailored to the victim.

The [e-mail sent](#) to Anastassiadis, CEO of Cyveillance, included his name, the company's name and even the correct phone number, said James Brooks, director of product management at the security vendor. "Given the nature of our business, he suspected something right away and forwarded it to our operations center."

However, [VeriSign Inc.](#)'s iDefense division has tracked more than 1,800 victims who clicked on the message. "This is probably one of the largest spear-phishing attacks we've seen to date in terms of number of victims," said Matt Richard, director of iDefense's Rapid Response Team.

VeriSign said the criminals behind this scam may be the same ones who launched an attack last month that used fake e-mails that appeared to be from the [Better Business Bureau](#). And the U.S. courts have been warning computer users for years now of an ongoing scam where victims are told that they have failed to show up for jury duty and then asked to enter sensitive information into a phishing site.

"The malware itself is not particularly interesting. It was clever that it went straight to CEOs and it didn't really blast the whole world," said [John Bambenek](#), a security researcher at the University of Illinois at Urbana-Champaign and volunteer at the [Internet Storm Center](#).

"For someone who doesn't know what a legal document looks like, it kind of passes the smell test," he added. "When they see they've been subpoenaed, people panic, and they click on things they shouldn't."

The mail directs the victim to a Web site that ends in "...uscourts.com" and is very similar to a legitimate .gov domain used by California courts, Bambenek said. The Web server delivering the malware is based in China, while the computer that then controls the victim's computer is based in Singapore.

The malware used in this scam was [not identified](#) by the majority of antivirus companies, although most were updating their software to flag it, Bambenek added.

By Monday afternoon, the Administrative Office of the U.S. Courts had posted [a note](#) to its Web site warning of the fake e-mails. "This is not a valid subpoena," said Karen Redmond, a spokeswoman with the office. "Subpoenas are not issued like that to individuals unless they're a party in the case."

The U.S. federal court system heavily relies on e-mail messages to help lawyers communicate with one another and the court throughout cases, and IT staffers in legal firms have traditionally had to work hard to make sure that these messages are not blocked by spam filters. Now they'll have one more thing to worry about: whether the court notices they're getting are legitimate notices or online attacks.

## Targeted Attacks Against Sensitive US Networks on the Rise (April 10, 2008)

BusinessWeek takes a look at the growing number of targeted attacks against US government and private industry systems. The problem is serious enough to have prompted the Cyber initiative, signed by President Bush in January, and reportedly a classified operation known as Byzantine Foothold, aimed at discovering the source of the attacks and protecting systems from attacks in the future. The Office of the National Intelligence Director responded to questions from BusinessWeek in writing, saying, in part, that "computer intrusions have been successful against a wide range of government and corporate networks across the critical infrastructure and defense industrial base." A Chinese government spokesperson denies the allegations that the attacks came from China, even though considerable evidence that shows the origin of the attacks exists. The article also goes into some detail regarding a targeted email sent to a Booz-Allen executive that contained malware known as Poison Ivy, a remote administration tool that is capable of logging keystrokes. Another piece of malware that accompanied the email is designed to disable security measures.

[http://www.businessweek.com/magazine/content/08\\_16/b4080032218430.htm](http://www.businessweek.com/magazine/content/08_16/b4080032218430.htm)

### "States Poised to Adopt Digital IDs"

Government Computer News (04/14/08) Vol. 27, No. 8 ; Jackson, William

It may only be a matter of years before states begin issuing electronic identifications, some experts speculate. Since the federal government now calls for employees and contractors to carry interoperable digital IDs, states, which "have always been the issuers of identity credentials," may soon follow, said Entrust's Peter Bello at the recent RSA security conference. "Maybe I'm being too optimistic, but I think it's just a matter of time," Bello says. He says states may start including them in the updated driver's licenses, or Real IDs, which are set to roll out in the next few years. "Having citizens access government applications is the next big thing." The digital certificates in the IDs could be interoperable with state and federal systems and also could be used to access commercial services.

### "Online Crime's Impact Spreads"

USA Today (04/11/08) P. B6 ; Swartz, Jon

Nearly 40 percent of Americans avoid online shopping and banking out of fear of identity theft, according to a recent TNS Sofres survey. F-Secure chief research officer Mikko Hypponen says international law enforcement agencies still do not have the resources to stop cyber crime and theft, which now accounts for \$200 billion in damages a year. However, he says the worldwide law enforcement agency Interpol still allots only about \$102 million toward combating criminal activities. Studies show consumers' fears are grounded in reality; according to a recent Symantec report, bank accounts were the most popular items for sale on underground computer servers, accounting for 22 percent of all sales in the last six months of 2007. Nefarious bots, or sprawling webs of compromised computers, attempt to lure in unsuspecting end users through excessive spam mailings that can number up to 100 billion messages a day, according to SecureWorks.

### "Storage: The New Frontier in Data Protection"

InternetNews.com (04/07/08) ; Mottl, Judy

The focus of IT security must move from peripheral approaches--protecting passwords, building firewalls, and fortifying networks--to storage-based solutions, says NetApp's Tim Russell. With a growing number of regulatory mandates, companies have more to lose by not protecting internal data. "The perimeter was once just the firewall, now it is moving closer to the storage environment," Russell says. "If you're not doing security there, you're going to have trouble because you're all letting more people into your networks and giving them more data access and security has to be in place." Russell says encryption technologies are the cornerstone for data security, although 75 percent of all data loss incidents still stem from human error. Massachusetts recently became the 39th state to introduce compliance laws for companies in regards to protecting personal information. In all areas of the country, failing to protect data not only threatens a company's reputation, but its finances. A Gartner study estimates a record breach costs an average of \$90 per record, while a Forrester report suggests the number is even higher, at \$305 per employee.

### "Whodunit? Stop These Employees From Leaking Your Corporate Data"

Computerworld (04/14/08) Vol. 42, No. 16, P. 26 ; McAdams, Jennifer

To mitigate the information security risks associated with vulnerabilities facilitated by employees, experts say companies should customize security plans according to individual employees. Similarly, businesses should avoid placing significant assets or information in the control of just one employee and management should refrain from being reluctant about

monitoring employees. As experts state that individuals are often the "weakest link" in IT security, security responsibilities should be distributed evenly across an organization. This will promote security from all aspects of a company while ensuring that no one employee retains too much authority in the area of security. Sufficient employee training remains the most effective way to account for optimum security, yet experts say that enterprises should take a more pro-active role in emphasizing the weight of IT security to employees. Beyond security training programs, experts say conveying to employees the possibility of losing their jobs due to a security breach is an effective way of underscoring the importance of security training.

## Security Manager's Journal: Enough of being the bad guy

Projects have gotten security reviews at the last minute once too often. Time for a new process.

By Mathias Thurman

April 21, 2008 (Computerworld) Security issues have a higher profile than they did a few short years ago, but too often, security managers still end up looking like the bad guy when they delay a project's go-live date. Never mind that the real cause of the delay is the failure of project managers to give security a thought until just before they plan to roll out the new application to users. It's the security manager who says, "No, this can't be used in our environment without a security assessment." It's the security manager who seems to have no compunction about negating months of hard work with orders for reworks that mitigate the security problems.

I've talked before about how frustrating this sort of thing is for me. A couple of weeks ago, it happened again. A workflow application had been in motion for almost six months, but I wasn't briefed until T minus 10 seconds.

### **TROUBLE TICKET**

**ISSUE:** Projects are frequently delayed because security isn't considered early enough.

**ACTION PLAN:** Change the process so that the security manager will no longer be the forgotten man.

I hate being hit with the same problems again and again, and I try to avoid that by thinking of ways to change our processes. So, after I did my review of the workflow application, I tackled the project life-cycle management process.

First, I reviewed all the projects from the past couple of years and categorized them according to type. Next, I defined several high-level criteria that dictate whether a project needs security consideration.

I came up with 13 criteria, including projects that involve new applications, partner connectivity, a merger or acquisition, software as a service, new network architecture, and the handling and transfer of personal information or financial data. Project managers can look over the criteria when they initiate a new project and quickly determine whether it will require security attention. If it does, I should be included as a member of the project team.

### **Baked-in Security**

I want the project team to be aware of what I expect before I sign off on a project. To this end, I created an easy-to-use spreadsheet of requirements that project managers can use to ensure that security is "baked in" early in the project's life cycle.

Each requirement gets a tab in the spreadsheet and is as generic as possible so that it's highly adaptable. The requirements include application security controls, partner connectivity requirements, merger-and-acquisition due diligence items and security requirements for application service providers offering SaaS. I have columns for the risks associated with noncompliance and for the suggested test activity. The spreadsheet should make it easy for teams to self-inspect the security posture of their projects.

Another important change is that I have been designated a definition-phase approver for every project. Now I will be notified of all projects early on. This will allow me to ensure that I am included in projects that meet my criteria, just in case a project manager neglects to review my criteria list.

Before receiving this Phase 2 designation, I wasn't brought into the loop until Phase 5, which is the operational-readiness phase that occurs just before go-live. With my involvement moved up to Phase 2, projects will actually have a better shot at going live on schedule.

On the governance end, I have created a new metric for tracking the percentage of projects that get operational readiness approval on the first try. My hope is that by measuring the effectiveness of this new process, project managers will see the value of bringing security considerations to the preliminary stages of initiatives.

I'll probably continue to tweak this new process, but I'm already confident that I am going to be the bad guy a lot less often.

## **Prevent identity theft by avoiding these seven common mistakes**

**Date:** April 21st, 2008

**Author:** Mike Mullins

Identity theft is on the rise. Is your organization part of the solution or part of the problem? Personally identifiable information (PII) is pouring through the security floodgates and ending up in the wrong hands at an alarming rate.

To protect your organization's employees and clients, you need to evaluate how well your company protects its PII. Here are seven common mistakes to avoid.

### ***Keep users in the dark***

Users will always be the weakest link in any enterprise network — and all of the gadgets and controls in the world won't change that. If your users don't know how to identify and handle PII, it's only a matter of time before one of them discloses this data to the wrong source.

The solution is simple: Educate your users on your company's policies and mechanisms to process PII. And don't forget to include regularly scheduled refresher courses.

### ***Partner with the wrong businesses***

You've made sure your security is rock solid, and you've trained your users. But can your business partners say the same? Do you collect or share information with businesses that have little or no security?

If your company collects and shares PII with insecure partners, who do you think will end up in the paper and explaining to law enforcement about how a breach occurred? Your company will.

The solution is just as simple as the last dilemma: Educate and train your business partners on how to protect this sensitive information. Charge them for your expertise if you want, but get the job done.

### ***Keep data around past its prime***

What do you do with data once it's served its purpose? If you aren't destroying PII when it's no longer required, then you're not doing your job. That doesn't mean throwing it away either — that means destroying it.

Dumpster divers make a living off of old bank statements and credit card receipts. That's why you need to wipe out PII when it's no longer necessary. If your organization doesn't have a shredder, you need to get one today.

### ***Don't worry about physical security***

It's imperative that you implement physical access controls to prevent unauthorized people — including employees — from gaining access to PII. Get a door lock and a badge reader, and start controlling access.

## ***Don't lock up your records***

If you don't have specific storage areas on your network (as well as file cabinets) for PII, then how can you properly protect it? Take inventory of your network — and your paper copies — and develop a plan to protect that data. This would be a good time to research encrypting data-at-rest and locking some file cabinets.

## ***Ignore activity on your network***

I've said this before in columns, but it's worth repeating: If you're not going to actively monitor your network for suspicious activity or incidents, then stop collecting the data. Develop a method that's within your capabilities and budget to monitor your network for suspicious activity or incidents. And while you're at it, develop a response and mitigation strategy for security incidents.

## ***Audits? Who needs audits?***

A lot of businesses either don't know what security events to audit or don't read their security logs — or both. If you're not sure which events to audit, [find out](#). Set up security auditing, and start reviewing your logs today.

## **Final thoughts**

Identity theft may be on the rise, but you don't have to make it easy for thieves. You can help prevent identity theft both at home and at the office — you just need to take a few extra steps.

## **NJ Supreme Court Upholds Reasonable Expectation of Online Privacy**

(April 21, 2008) The New Jersey Supreme Court has ruled that Internet service providers (ISPs) cannot release personal information about their customers without valid subpoenas. The unanimous ruling upheld lower court decisions that related to police seeking the identity of a woman suspected of accessing her employer's computer system. The police had a subpoena from a municipal court, but because the alleged crime was an indictable offense, the court required a grand jury subpoena. This is "the first ruling in the nation to recognize a reasonable expectation of privacy for Internet users."

<http://www.phillyburbs.com/pb-dyn/news/104-04212008-1522473.html>

<http://blogs.usatoday.com/ondeadline/2008/04/nj-high-court-e.html>

[http://www.nytimes.com/aponline/technology/AP-Internet-User-Privacy-](http://www.nytimes.com/aponline/technology/AP-Internet-User-Privacy-Ruling.html?ei=5088&en=17282b829d347c4b&ex=1366516800&partner=rssnyt&emc=rss&pagewanted=print)

[Ruling.html?ei=5088&en=17282b829d347c4b&ex=1366516800&partner=rssnyt&emc=rss&pagewanted=print](http://www.nytimes.com/aponline/technology/AP-Internet-User-Privacy-Ruling.html?ei=5088&en=17282b829d347c4b&ex=1366516800&partner=rssnyt&emc=rss&pagewanted=print)

[Editor's Note (Schultz): This is a very significant victory for privacy advocates, but if this case goes to the Supreme Court, I would not count on the ruling being upheld.]

## **No suspicion needed to search laptops at U.S. borders, says Ninth Circuit**

### **Ruling blow to privacy rights of travelers**

**By Jaikumar Vijayan**

April 22, 2008 (Computerworld) In a ruling that's likely to come as a disappointment for privacy rights advocates, the [U.S. Court of Appeals](#) for the Ninth Circuit this week held that customs officers need no reasonable suspicion to search through the contents of any individual's laptop at the country's borders.

The ruling reversed an earlier decision by the U.S. District Court for the Central District of California, which had granted a motion seeking to suppress evidence gathered from such a search in a case involving child pornography. In arriving at that decision, the district court ruled that customs officers indeed did need to have reasonable or particularized suspicion for searching through laptops at U.S. borders.

The case involves a man named Michael Arnold, who was arrested in 2005 on charges of transporting child pornography on his laptop. According to a description of the case in court records, Arnold was returning home from a three-week vacation in the Philippines in July 2005, when he was pulled aside for secondary customs screening at Los Angeles International Airport.

A customs officer who was inspecting Arnold's luggage asked him to start his computer and had it examined by colleagues who found several images of what they believed were child pornography on the computer and in several storage devices that Arnold was carrying with him.

A grand jury later charged Arnold with knowingly transporting child pornography in interstate and foreign commerce, and for knowingly possessing a hard drive and CD-ROMs containing more than one image of child pornography.

Arnold filed a motion asking for the evidence against him to be suppressed, arguing that the search of his computer and storage devices by customs officers had been unreasonable and unwarranted. The district court ruled in his favor on the grounds that reasonable suspicion indeed needed to have existed for customs officials to have conducted the search.

The government filed an appeal against that decision essentially arguing that reasonable suspicion standards did not apply to searches at the border.

In concurring with that view, the Ninth Circuit yesterday rejected Arnold's arguments that reasonable suspicion was needed to search a computer because of its ability to store large amounts of data, ideas, e-mail, chats and Web-surfing habits. It also rejected Arnold's argument that a higher level of suspicion was needed for computer searches at the border because of the risk of "expressive material" being exposed in such searches.

"We are satisfied that reasonable suspicion is not needed for customs officials to search a laptop or other personal electronic storage devices at the border," noted Judge Diarmuid O'Scannlain, who wrote the opinion of the three-judge panel.

In writing the opinion of the appeals court, Judge O'Scannlain cited numerous cases to show that courts have long upheld suspicion-less searches of closed containers and their contents at U.S. borders. These include searches of items such as a traveler's briefcase, purse, wallet or pockets. Citing one such case, Judge O'Scannlain noted that generally, "searches made at the border ... are reasonable simply by virtue of the fact that they occur at the border."

O'Scannlain noted that the Supreme Court has called for a reasonable-suspicion standard for certain types of border searches such as those that could cause exceptional damage to property or those conducted in a "particularly offensive manner." Neither of those situations applied in Arnold's case, he said. He also pointed to a decision by the Fourth Circuit Court of Appeals upholding the warrant-less search of a vehicle that was entering the U.S. from Canada.

In that case, the search resulted in the discovery of a videotape -- and, subsequently, other material -- suggestive of child pornography. As a result, the Fourth Circuit Court held that warrant-less searches were OK because requiring otherwise would have imposed an "unworkable standard" on customs officials. "We are persuaded by the analysis of our sister circuit," O'Scannlain wrote.

The Ninth Circuit Court's ruling comes amid growing concern over the issue of laptop searches at U.S. borders.

In February, the Asian Law Caucus (ALC) and the [Electronic Frontier Foundation \(EFF\)](#), two San Francisco-based civil liberties groups, filed a lawsuit in California citing complaints from travelers of excessive screenings at border entry points, including inspections of the data on laptops, cell phones and other electronic devices.

The lawsuit was filed in [U.S. District Court](#) in San Francisco. It asked the court to order the [U.S. Department of Homeland Security's](#) Customs and Border Protection (CBP) division to release records relating to its policies and procedures relating to such screenings and searches. In the complaint, the ALC and the EFF noted that they had heard from travelers who claimed that CBP staffers inspected and sometimes copied the contents of their laptop files and cell phone directories without providing any reason for doing so.

## Q&A: Schneier says cybercrime problem 'might not be fixable'

Business changes are needed to combat identity thieves, BT Counterpane CTO contends

By Jeremy Kirk

April 22, 2008 (IDG News Service) [Bruce Schneier](#) is an expert on cryptography and a well-known author and [commentator](#) on information security issues in general. [Schneier](#) also is chief technology officer at BT Counterpane, a managed security services vendor that is part of [BT PLC](#); the company was founded by Schneier as Counterpane Internet Security Inc. in 1999 and then [acquired by BT](#) in October 2006. At the Infosecurity Europe 2008 conference in London this week, Schneier spoke with the [IDG News Service](#) about the psychology of data security and the effectiveness of security software. Excerpts follow:

**Are antivirus vendors just making money by giving people [a feeling of security](#) instead of real security?** Antivirus products actually work; they have for years. A lot of the software on this show floor is just snake oil, but antivirus does work. You should have an antivirus program; you should have it updated regularly. It doesn't make you secure, but it gets that bottom layer of the trivial stuff. It's not sufficient, but it's certainly necessary.

**People are tricked into [downloading malicious software](#) through social engineering. Have people become so conditioned — mainly by watching television — that they believe whatever appears on their PC monitors?** Yes, but it's not television. People believe what they see on the Net not because of television but because of the [trappings of reality](#). So when you got to BT.com, you see the BT logo, the BT font, the PR material, and you think, "Yeah, it's BT" — like when you go to your bank, you see the logo and the tellers.

On the Web, it could be a fake BT.com site and you don't notice, because it's trivially easy to copy. So people do believe what they see on the Internet — not because of television, but because the Internet has the trappings of the real world. All of those social cues you get to know to trust something — it [looks professional](#), nothing's misspelled — you see those things and you believe it's real.

**Do you think people will ever become more suspicious of the Internet?** Younger people will pick it up. But certainly you can always fool people unless there is some external validation of [Web sites]. Unless you can do that, there's no guarantee that [users] are not going to be fooled.

**What do you think the biggest online threat is right now?** Crime.

So how do you fix it? It's expensive to investigate, and it's cross-jurisdictional. It might not be fixable. A lot of [the solution] is going to be making the things that criminals are going after harder to get. You're not going to stop the criminals [from trying]. But in the United States, it's really easy to get a credit card in someone else's name. The credit card companies like it that way. So a lot of it is looking at how the criminals [are attacking things](#) and making it harder [for] them. The brokerage companies want it to be easy for you to log on and make trades. Make it harder, and the businesses don't like that.

**They're afraid that it will drive away customers.** Of course. If I strip-search you before you go into the bank, you might change branches. In the U.S., the government doesn't have the [guts] to require stuff like [stronger authentication]. You've got to make the banks responsible for losses. The brokerage company has to [reimburse] me if I didn't make a [fraudulent] trade — period, end of sentence. That's how you fix it. Because then, my brokerage is going to start buying security; otherwise, they won't.

The basic rule of security: you make the entity in the best position to mitigate the risk [responsible](#) for the risk. Make them responsible — they'll figure it out. That's how capitalism works.

# The darker side of Webmail

Web-based e-mail may be exposing you to privacy and security problems you didn't expect

By Tam Harbert

April 28, 2008 (Computerworld) Web-based e-mail is booming. Services such as [Gmail](#), [Yahoo Mail](#) and Hotmail are convenient, accessible and, best of all, free. Many of us have come to rely on them without giving it a second thought.

But second thoughts may be in order, according to security experts, privacy advocates and some Webmail users. Few consider the fact that Webmail is inherently different than POP3 e-mail. It differs in who administers it and how, in the ways it may be vulnerable to hacking, and in the type of help you can expect when you have a problem.

You may not think these differences matter. And they don't -- unless they end up biting you in the backside. For example, the most popular Webmail services are prime targets of malicious hackers. Some Webmail users run into mysterious technical problems that are never explained or solved. And most Webmail users never really know where their data is being stored or for how long -- or how well it is being safeguarded.

## How private is Webmail, really?

Although Webmail is often billed as a free service, the old adage "you can't get something for nothing" definitely applies here. While you're not giving the Webmail provider any of your cash, you are making a trade: Your personal information in exchange for the service.

When you click that box on the licensing agreement -- you know, the one you didn't read -- you're probably giving permission to use the personal information you entered when you signed up. For example, [Google Inc.'s Privacy Policy](#) specifically states that it collects personal information such as your name and e-mail address; it also collects information collected through your browser (such as which sites you visit) and from the text of your e-mails, which the provider uses to customize ads and conduct research.

## Most Webmail users never really know where their data is being stored or for how long -- or how well it is being safeguarded.

"It's all about accumulating information about the user," notes Rob Douglas, a privacy and security consultant who edits [InsideIDTheft.info](#). "Sure these services are 'free,' but the trade-off is that they are obtaining information about you that has value in the world of advertising and marketing." (Admittedly, most of the time this information is collected in the aggregate, so that no individuals are actually picked out.)

Not too worried about that? Maybe you should be. "I believe individuals tend to forget that much of what they do online is being recorded," says Douglas. "This collection of information is all done behind the scenes; it's not visualized when individuals are using their computers."

It can be shocking to realize how much about yourself you reveal on the Web, particularly when vendors combine information from your Webmail account with other Web 2.0 sites, such as online social networking platforms. "You start to leave a trail of information about yourself on the Internet," says Stephen Northcutt, president of the [SANS Technology Institute](#). "Do you really want to get ads on burial plots because you drink, smoke and engage in unprotected sex?"

## Showing others your e-mail

It's fairly easy (if you know how) to gain access to and read others' Webmail without permission, either legally or not, notes [Jeremiah Grossman](#), founder and chief technology officer at [WhiteHat Security Inc.](#), which tests Web sites for vulnerabilities. "Webmail should never be considered private, ever," he says. "It can be read in many, many different ways," including rogue customer service reps at the e-mail provider, law enforcement with a subpoena or a national security letter, or a curious hacker sniffing packets on the Internet.

It was simple for the SANS Technology Institute to get a subpoena when it noticed a Gmail user was stealing its exam questions and posting them on the Internet, says Northcutt. People think that just because they don't use their real name or identifiable information in their e-mail sign-on -- using some obscure jumble of numbers and letters instead -- that no one can tie it back to them. "Of course, we can," says Northcutt. For example, an ISP can be subpoenaed to reveal the contact information that a person used when signing up for the account.

## WHAT'S YOUR WEBMAIL'S PRIVACY POLICY?

Those of us who spend a lot of time working with online and offline technology tend to shrug when confronted with bothersome details such as manuals, EULAs, and privacy policies. However, if you take a few minutes to really read them, you may find that the privacy policy of your Webmail service provider may include a few provisions that you want to at least be aware of.

Here are links to the privacy policies of the Big Three Webmail providers -- [Google](#), Yahoo, and Microsoft -- together with a sample of what they contain. Forewarned is forearmed.

- [Google Privacy Policy](#)  
**Sample clause:** "When you sign up for a Google Account or other Google service or promotion that requires registration, we ask you for personal information (such as your name, email address and an account password). For certain services, such as our advertising programs, we also request credit card or other payment account information which we maintain in encrypted form on secure servers. We may combine the information you submit under your account with information from other Google services or third parties in order to provide you with a better experience and to improve the quality of our services. For certain services, we may give you the opportunity to opt out of combining such information."
- [Yahoo Privacy Policy](#)  
**Sample clause:** "Yahoo! collects personal information when you register with Yahoo!, when you use Yahoo! products or services, when you visit Yahoo! pages or the pages of certain Yahoo! partners, and when you enter promotions or sweepstakes. Yahoo! may combine information about you that we have with information we obtain from business partners or other companies."
- [Microsoft Online Privacy Statement](#)  
**Sample clause:** "Microsoft collects and uses your personal information to operate and improve its sites and deliver the services or carry out the transactions you have requested. These uses may include providing you with more effective customer service; making the sites or services easier to use by eliminating the need for you to repeatedly enter the same information; performing research and analysis aimed at improving our products, services and technologies; and displaying content and advertising that are customized to your interests and preferences."

Or it could be the [FBI](#) looking for terrorist activity. Under the [USA Patriot Act](#), the FBI can use a national security letter to get telecommunications records, including e-mail records. A recent report from the Justice Department's Office of the Inspector General titled "[A Review of the FBI's Use of National Security Letters](#)" (PDF) found that the FBI has, in some cases, misused these surveillance powers. It also found that some e-mail providers were handing over full message bodies and subject lines of e-mails when they were really only supposed to hand over billing records.

"If you read the fine print in end-user license agreements, there's always the possibility for the government to intervene," says Larry Ponemon, founder and chairman of the [Ponemon Institute LLC](#), a privacy and information management research firm.

Google's policy, for example, is to notify an e-mail user when the government orders it to turn over records, "except in cases where we're not legally able to do so because notification threatens to impede a law enforcement investigation," says a Google spokesperson.

This isn't a theoretical problem. Back in 2006, Google was [served with a subpoena](#) from the DOJ: The DOJ wanted two months' worth of search queries from users, together with as many as 1 million Web addresses, to bolster its arguments in a Pennsylvania pornography case. After some legal back and forth, it was [finally decided in March 2007](#) that Google did have to supply the DOJ with 50,000 Web addresses, but not any of the user search queries.

Google isn't the only Webmail supplier that has found itself in the courts. For example, in April of 2006, an ex-employee's Yahoo e-mail account was [successfully subpoenaed](#) by his former employer. And Yahoo made headlines when news organizations reported that the company [had handed over](#) the contents of personal e-mail accounts to the Chinese government, resulting in the arrest and imprisonment of several Chinese dissidents.

### A corporate security tangle

The increasing popularity of third-party Webmail also presents new and sometimes poorly understood security problems for corporate IT departments.

Most corporate e-mail travels through an SMTP server, which typically scans incoming e-mail and attachments for malware and inspects outgoing mail for any violations of corporate policy. Not so with Webmail, which goes through the corporate HTTP server and is usually not inspected on its way into the network, notes Chenxi Wang, an analyst at [Forrester Research Inc.](#) That means Webmail can bring in security threats and send out sensitive corporate data.

"Unless you've got scanning in place there, it's a huge hole for corporations," says John Maddison, general manager of Trend Micro Inc.'s network security services group.

Some corporations sabotage themselves through ignorance or misguided policies. A company might forbid the use of corporate e-mail for personal business, leaving employees little choice but to use their Webmail accounts. Even without a formal policy, "people might think it's the right thing to use their Gmail account for personal business rather than to use their corporate e-mail," says Ponemon.

Some e-mail providers were handing over full message bodies and subject lines of e-mails when they were really only supposed to hand over billing records.

In other cases, a company might make employees jump through so many security hoops to access their e-mail remotely that they use Webmail instead, says David Cowings, senior manager of operations in security response at [Symantec Corp.](#) For example, employees might forward copies of inbound corporate e-mail to their Webmail account rather than go through a complicated process such as using a rotating access key to dial in through a VPN from home or while traveling. Or perhaps corporate IT limits the size of attachments, so if employees need to send a 2M file, they turn to Webmail, says Frank Cabri, vice president of marketing and product management at [FaceTime Communications Inc.](#), a security vendor that specializes in securing noncorporate-sanctioned applications like Webmail.

Indeed, when companies start to look at what's traveling through their HTTP channel, "usually IT people are very surprised at the extent of this unsanctioned traffic," Cabri notes.

On the other hand, the dynamic nature of Webmail can be a security plus, says Jen Grant, a group product marketing manager at Google. "The advantage of Webmail and the [cloud](#) is that we can adapt and adjust almost instantaneously, so the second a new type of malware is there, we can adapt, adjust and update our system and protect our users," says Grant. Contrast that with a static system on a corporate desktop, she says. "In order for them to adapt, they have to download something, they have to install something. It's just not as fast."

Webmail isn't necessarily any more vulnerable than corporate mail, says Petko D. Petkov, founder and senior security consultant at [Gnucitizen](#), which does [penetration testing](#) for companies. Although directly attacking corporate e-mail systems is harder, there are other ways to break into the system, through social engineering or sniffing unprotected wireless connections of corporate laptops at Starbucks, for example. "There are so many variations," he says. "It's just a matter of creativity and innovation."

### **Webmail is different**

However, there's no denying that Webmail, because it is a Web application, is subject to attacks from black-hat hackers looking for vulnerable targets. "It's the law of large numbers," says Ponemon. "The seriously bad criminals -- computer jocks in places like Romania and China -- they look for the big brands because that's where they'll get the most traction from their criminal activity."

The two most prevalent vulnerabilities today are cross-site scripting and cross-site request forgeries, according to Petkov. In fact, cross-site scripting is the most prominent vulnerability on the Web, notes Grossman. "It's what's used most often to break into Webmail accounts specifically."

In Webmail cross-site scripting, a cybercriminal will send an e-mail that contains some malicious HTML and JavaScript code in it. When the victim opens that Webmail message, the code automatically executes and sends their cookies, which contain the information needed to get access to that Webmail account, back to the bad guys. Once that happens, the criminals "have everything they need to log in as you," says Grossman. "There's not much you can do about it."

Cross-site request forgery uses cross-site scripting as its first step, says Petkov, but it goes further and uses that info to impersonate the victim to gain access to other accounts. Last fall, Petrov reported [a Gmail vulnerability](#) that could allow a hacker to use cross-site request forgery to log into your e-mail account and configure it to forward copies of all your e-mails to the attacker's address. Or they might configure it to simply send copies of all e-mails that contain words like "account number" or "password," which might deliver the information needed to sign into the victim's bank account. Most users would never even realize this was happening -- that is, until they logged into their bank account and found it had been drained.

Google fixed the vulnerability (although, according to Petkov, it wasn't a complete fix and some users were compromised). And Petkov isn't singling out Google for special criticism. All Webmail vendors are engaged in a constant battle against these and other types of exploits, he says. "I'm sure Google is putting a lot of effort into securing their software, but mistakes

happen," Petkov notes. "Especially on the Web, where everything is constantly changing and people are always striving to add new features. Every time they add a new feature, there could be a problem."

### **This is your life on a server**

Finally, what can you do if you have a problem with Webmail? For example, if your e-mails disappear.

That's what happened to Jeneane D. Sessum, a writer and consultant in Atlanta who uses Gmail and several other Google Web-based applications. Last November, a large chunk of the e-mail messages she had stored on Google's server [simply disappeared](#). When she tried to contact Google support, she was directed to its online help forums. She couldn't find an answer there. Then she filled out a contact form to report a technical problem. In reply, she received a form e-mail saying that Google had determined that there was no outage or data problem that would have caused her e-mail to vanish. "That was it," says Sessum. "No advice on what to do." She had to work through her own personal network to reach an actual person at Google, someone in technical support. "But still nobody could tell me anything except that nothing was wrong on their end."

## **HOW TO PROTECT YOURSELF**

**Do:** Use a strong password that is unique to your e-mail account and change it frequently. (You can use services such as Security Stats Com's [Password Security](#) Web applet to check your password's effectiveness.)

**Do:** Change your password and contact the Webmail provider immediately if you suspect your account has been hacked or hijacked.

**Do:** Keep a separate backup of your Webmail. One way is to configure your Webmail to forward a copy of everything to another e-mail account. In addition, Google offers instructions on how to [back up your e-mail](#) to your POP3 e-mail client.

**Do:** Find out how the service provider protects your data in transit and in storage. For example, does it provide an option to use SSL encryption when sending an e-mail? Does it encrypt the data on its servers? Are there backups in case those servers fail?

**Don't:** Use your Webmail address as a sign-on for other accounts. If you do and your Webmail is hacked, then the hacker will automatically have access to those other accounts.

**Don't:** Use your Webmail as storage for your old e-mail unless you're completely comfortable doing so. You're better off backing up your e-mail to a local hard drive and then deleting it from the service.

**Do:** Be cautious when checking your Webmail on public terminals in places like airports, libraries, etc. Make sure you haven't left any cookies and clear your private data (such as cache and browsing history). And remember that your work computer is not private.

**Do:** Use a secure HTTPS connection whenever possible.

Sessum wishes Google could be more responsive, especially to users like her who are basing their small businesses on its platforms. "I don't buy this line that these are free services and so you get what you pay for," she says. "They make money off of me by serving ads up every time I send an e-mail." She says she'd gladly pay Google some type of premium fee that would get her better support and perhaps guaranteed backups of her e-mail.

Google's Grant won't discuss individual problems like Sessum's, citing user privacy. Google can sometimes restore deleted e-mail, she says, depending on how much time has passed. Ultimately, Google permanently deletes it, but she won't specify the amount of time that Google waits before doing that. "We must strike this balance between, on the one hand, keeping that e-mail around just in case of situations like this so that we could recover the e-mail for the user and, on the other hand, doing what the user has told us to do when they tell us to delete the e-mail," she says.

Tellingly, Sessum still uses Gmail and her other Google apps. Indeed, most users seem willing to accept the trade-offs in exchange for the features, usability and accessibility of these services.

Sessum, for example, admits that she should have been more conscientious about keeping her own backup of her Gmails. Ironically, she's configured her Gmail account to forward a copy of everything to her Yahoo Mail. "So my backup to my Web-based e-mail is another Web-based e-mail account," she admits.

## Eight Surefire Ways to Become an Identity Theft Victim

**Practice unsafe surfing.** When you purchase a new computer, go online without activating the firewall, or purchasing protective software.

Further expose yourself digitally by sharing a wireless connection with the entire neighborhood. Without digital encryption, you can share the contents of your hard drive with anyone on the street. For maximum risk, do some online banking on a public computer -- like the one at the library or a public cafe. Bonus points are added if your Social Security number is your user ID for any transactions.

**Skimp on anti-virus and anti-spyware protection.** Courting disaster online is easy. Invite malicious code to attack your computer simply by doing nothing. Antivirus programs can be pricey, and the maintenance of constantly downloading updates is time-consuming. Combine that with the security updates from Microsoft or Apple and it's enough to seriously annoy anyone.

**Passwords are a pain!** Make life easy for yourself by using the same password for EVERYTHING, and make it something easy to remember, like your first name or 'password'. Just in case, make sure you write it down on a yellow sticky and put it somewhere easy to see.

And don't forget to have your browser set to 'remember password' to make life easy for you - and the cyberthief.

**Peek at junk email and open attachments from unknown sources.** Open attachments from strangers, secret crushes, long-lost friends saying "what's up," or strangers hawking cheap drugs -- you'll never know unless you peek at that email. One of the many fun things that can happen when you open an attachment containing malicious code is infecting your computer with a Trojan horse or virus, which can easily lead to identity theft.

**Stuff your wallet with juicy identifying tidbits.** Wallets and purses are more than just handy cash-carrying devices. They often have credit cards, identification, insurance information and even Social Security cards. Obviously, more is better if you'd like to become the prey of fraudsters. Losing or misplacing a wallet or purse can cause more problems than just the hassle of replacing all those cards and buying a new bag. Armed with your date of birth, Social Security number and mailing address, there's no limit to the damage thieves could cause.

**Make your checks payable to criminals.** If you're like most people, you wouldn't post your checking account information on your front door, though you should if you'd like to be a victim of fraud. Similarly, checks reflecting the same information can be dropped casually into unsecured mailboxes. Statistically the chances of your mailbox being targeted by criminal elements are low, but not that low. According to the 2008 Identity Fraud Survey Report from Javelin Strategy and Research, almost 1 in 10 victims of identity theft who can pinpoint the scene of the crime say that it happened at the mailbox.

**Opt out? Opt in!** While you're mailing checks from the unlocked mailbox, go ahead and get credit card companies to send you all the pre-approved offers that the postman can cram into the box. Similarly, don't get credit card statements online; leave them on the side of the road so that they're more convenient for fraudsters who lack the technical knowledge or follow-through to launch complicated hacking schemes.

**Nothing is too good to be true.** Everyone wants to feel special and maybe more importantly, filthy rich. When reading an emailed proposition from an African business tycoon, an imperiled prince or downtrodden heiress offering millions of dollars in exchange for some small measure of assistance, it's difficult not to wish it were true. Falling for the story will undoubtedly lead to unpleasantness.

## Employees Find Ways to Skirt Enterprise Security

### Applications that enterprise IT does not support create risk for the business

[Katherine Walsh](#) April 24, 2008

Enterprise users are "actively and intentionally" evading IT security controls and ignoring acceptable use policies, according to Palo Alto Networks' first annual "Application Usage and Risk Report."

The recent survey results from Palo Alto, a firewall vendor, are based on traffic from 350,000 users in 20 organizations that span the financial services, manufacturing, healthcare, state/local government and healthcare industries.

The report highlights applications (not generally supported by enterprise IT) that employees are actively using, as well as the major risks associated with their use.

Among the findings:

- External proxies that IT does not support, such as CGIProxy and KProxy, were present in 80 percent of the customer networks
- Web-based file transfer and storage applications such as YouSendIt and MediaMax were detected in 30 percent of sites
- Over 50 percent of applications using port 80 (the default port number for a web server) were not business related
- [Google](#) applications were found in 60 percent of the sites using port 80
- Web video and streaming audio consumed significant bandwidth on 100 percent and 95 percent of the sites sampled, respectively
- Peer-to-peer file sharing applications were found on 90 percent of the sites

Associated risks include:

- Data loss through unmonitored and/or unauthorized file transfers
- Compliance violations, both with internal policies and external regulations
- Business exposure from malware propagation or application vulnerability exploits
- Operational cost increases due to higher bandwidth consumption and added IT expense
- Lost productivity from excessive use of personal applications

## Unsecured USB Flash Drives Still a Risk, Survey Shows

Access Control & Security Systems (04/22/08)

IT managers are ignorant about the rampant usage of personal USB flash drives in the workplace. In a SanDisk survey of both end users and IT managers, respondents estimated only 35 percent of corporate end users use their personal drives at work. In reality, 77 percent of corporate end users use their own personal drives in the office for work-related purposes. Some of the files most likely to be copied onto personal drives include customer records (25 percent), financial information (17 percent), business plans (15 percent), employee records (13 percent), marketing plans (13 percent), intellectual property (6 percent), and source code (6 percent). Most companies have policies and endpoint security solutions in place to prevent data theft by employees, but only 57 percent train employees once or several times a year. Twenty-two percent of employers give training only once when hired, 17 percent provide training as needed, and 3 percent of companies say they still do not train employees on information security.

## Understanding Data Security Risks of P2P

### Companies face unexpected risk of data loss from employees using peer-to-peer networks.

Peer-to-peer file transfers are increasingly a source of data leaks, and IT organizations may not be appreciating the risk.

According to a survey by the Ponemon Institute of 750 IT professionals released the week of April 21, although 63 percent of respondents said their organizations forbid the use of P2P applications, only 5 percent said their organizations monitor P2P networks for data leaks. Twenty-six percent admitted they were unaware of any policies regarding P2P applications.

The problem was underscored in 2007 when a former employee of Citigroup's ABN AMRO mortgage group leaked the personal information of 5,000 people via a P2P messaging network. Pharmaceutical giant Pfizer also experienced a breach courtesy of a P2P application that exposed the personal data of 17,000 people.

Tiversa, which sponsored the study and monitors P2P networks, reported that the previous week it had uncovered W2 forms for 2,498 employees of a company coming from that company's own network. The user in that case was on the Gnutella network using LimeWire, and while the organization had a policy against P2P usage, the employee disregarded it, said Robert Boback, CEO of Tiversa. Adding to the issue is that peer-to-peer networks are typically designed to circumvent firewalls and go over Port 80 instead of other monitored ports, he said.

"Our research shows that the highest time of use is during the U.S. work day—these aren't kids downloading files at night; P2P users are often individuals at work taking advantage of their high [bandwidth](#)," Boback said. "For many companies that have put security measures in place, we still find files disclosed from their internal corporate IP range because P2P is very good at getting around IT measures."

In addition, files coming across P2P can be disguised to look like legitimate MP3s but instead be Trojans. Paula Skokowski, vice president of marketing at secure file transfer vendor Accellion, said [spyware](#) and [viruses](#) transmitted via P2P file sharing can spread very rapidly and widely among users.

There is of course a simple answer to the problem—block P2P applications. However, Gartner analyst Peter Firstbrook noted that it is not easy to block all of them, and users actively look for ways to avoid the blocks, such as using laptops when they are out of the network. In addition, [data](#) loss prevention tools are not widely deployed, he said.

"[DLP tools] are mostly just monitoring versus blocking to avoid blocking legit [business](#), so it is a bit like [closing] the proverbial barn door after the horse," Firstbrook said. "A well-configured DLP solution should catch P2P leaks, but that is not deployed in most organizations."

For companies, anywhere from 40 to 60 percent of the confidential files disclosed on P2P file-sharing networks originate from sources outside the corporate perimeter, such as suppliers, contractors, attorneys, partners, and employees working from home or on the road, Boback said.

"These endpoints are almost impossible for a company to control," he said, referring to those third-party sources as the extended enterprise. "An organization must take an extended enterprise view because very often the information custody chain extends outside their four-walled perimeter [security](#) approaches."

## PCI Update Requires Both Network and Application Penetration Testing

April 22 2007 - The Payment Card Industry Data Security Standards, which are being closely followed by tens of thousands of governments and commercial organizations and schools around the world, were updated to clarify what the required penetration testing must cover: "Penetration testing is different than the external and internal vulnerability assessments. A vulnerability assessment simply identifies and reports noted vulnerabilities, whereas a penetration test attempts to exploit the vulnerabilities to determine whether unauthorized access or other malicious activity is possible. Penetration testing should include network \*and\* application layer testing as well as controls and processes around the networks and applications, and should occur from both outside the network trying to come in (external testing) and from inside the network.

## DIY identity-theft protection: A 12-step program

Like changing your own oil, digitally speaking

By Dan Tynan

May 6, 2008 (PC World) - You don't have to spend \$100 to \$200 a year to defend yourself from identity theft at the level of protection that a paid service offers. You can do almost everything the services do, for free. But following these steps will require time and effort.

1. Get a free copy of your credit report by visiting AnnualCreditReport.com. Don't be fooled by look-alike sites that promise free reports if you subscribe to their credit-monitoring services. Better yet, order by phone at 877-322-8228.
2. For DIY credit monitoring, order a free report every three months from a different bureau. Scan the report for unfamiliar information, such as accounts you don't remember opening.
3. Place a fraud alert on your credit report by calling one of the credit bureaus. (You can find contact information for all three bureaus by browsing to Fight Identity Theft.)
4. Put a recurring event in your online calendar to remind you to renew your fraud alert in 90 days.

5. Tell the bureaus to stop selling your information to credit services, by calling 888/567-8688 or visiting [OptOutPrescreen.com](http://OptOutPrescreen.com). Doing so will reduce but not eliminate the number of preapproved credit card offers you receive.
6. Request a free public records report from ChoicePoint. You'll have to print a form and mail it, along with copies of your driver's license and proof of address. Scan the report for addresses and other details not related to you.
7. Take your name off other marketing lists by signing up for ProQuo.com's free service. In some instances, you may have to mail letters or navigate to a marketer's own site to complete your opt-out request.
8. Buy a mailbox that locks, or use a post office box. This will help prevent thieves from stealing your identity via paper mail.
9. Buy a crosscut paper shredder and shred junk mail to frustrate dumpster-diving identity thieves.
10. Never click a link from an e-mail message to log in to your bank or to any other financial institution. Type the secure site's address into your browser, bookmark it, and use that link to access your accounts. Otherwise, you risk having your identity stolen by phishers.
11. If you believe that you are a victim of identity theft, contact the Identity Theft Resource Center. Volunteers there can walk you through the process of restoring your identity.
12. Get educated. Mari Frank's [IdentityTheft.org](http://IdentityTheft.org), the Privacy Rights Clearinghouse, and the Federal Trade Commission maintain huge libraries of information on how to avoid being victimized, and what to do if it has already happened.

## **PDA's and labor laws**

**Date:** May 6th, 2008 -Toni Bowers

The Canadian paper *The Globe and Mail* ran a story last week in which it stated that a union representing government workers was going to make [the use of pocket-size electronic devices such as BlackBerrys a bargaining issue](#). In other words, it's advocating that the government pay its employees for work they do out of the office.

From the article:

"For some people, having a BlackBerry is like: We own you. You are our person, 24 hours, 7 days a week," said Ed Cashman, Public Service Alliance of Canada's regional executive vice-president for the National Capital Region, who says the union will insert the issue of BlackBerry use into its continuing contract negotiations.

In the United States, legal experts are warning that a new wave of overtime litigation is on the horizon, in which employees will claim overtime for all the hours they've spent clicking away at their hand-held devices.

Some experts believe that adding PDA usage to contract negotiations would result in people working longer hours or would add more expectations around availability. Some say it's up to the individual to just turn the device off.

## **"White House BlackBerry Breach a Wake-Up Call"**

**[InternetNews.com \(04/28/08\) ; Mottl, Judy](#)**

The potential exposure of political information from stolen BlackBerrys has highlighted the need for reinforced security in portable devices. Two of the smart phones in the possession of U.S. diplomats were reported missing; the White House has not commented whether or not the devices contained sensitive information or the possibility that the information was exposed. Research In Motion's Scott Totzke says the possible breach represents a significant warning for companies. Totzke urged enterprises to establish and enforce wireless security policies, a move that has been observed by the BlackBerry maker following a revised release of its expanded security policies in January. The smart phones are equipped with a number of security features, including two-factor authentication enabling and the ability to self-destruct after excessive password attempts. BlackBerrys also come equipped with a feature that allows IT staff to eradicate all information on the phone, if necessary. Totzke noted that in the current security climate, there is a greater necessity to strengthen technology beyond passwords and employ more infrastructure-related mechanisms for safeguarding storage devices.

## **"Wireless Vulnerabilities Present Enterprise-Wide Threats, Expert Says"**

**Dark Reading (04/28/08) ; Wilson, Tim**

Wireless Internet access is still in the infant stages of security, much like the Internet was when it was first introduced, says AirPatrol CEO Nicholas Miller, a participant at the April Interop/CSI SX Conference. "The problem is that wireless vulnerabilities don't just expose the user who's unaware of them, but the whole corporate network the user is attached to," Miller says. Companies save money on infrastructure and equipment by switching to wireless networks, but Miller says security managers often make the transition backwards and fit a security system onto a network retroactively. Instead, he says IT managers should implement a wireless security system first, and then install the access points and tools that fit into the security system. "You don't need all of that complex wireless technology if you have a wireless threat management system in place with encryption and security," Miller says.