CCC News:

Control Computer Crimes

Issue 0013 - 31 December 2009

Message from the Editor

Welcome to the Thirteenth issue of CCCNews Magazine.

This is the last issue for the year 2009. As happens every year, there are lots of predictions for the security scenario and risks, which will prevail in year 2010. We are giving you four reports on these predictions for security vulnerabilities in 2010 by various authors. These have been selected from over 15 reports and look more appropriate.

Further, one risk, which has not been covered in any of the predictions is breaking of cryptographic algorithms. In the last few days, three major incidents happened regarding breaking of encryption algorithms, all in 26th Chaos Communication Congress (26C3).

Unless, a more robust encryption algorithm is devised or invented, all 64, 128, 256 bit encryption will gradually be broken, given the computing power and grid computing. The world will be at the mercy of hackers. There will be rarely secure transaction. Thus, the new algorithm must be robust, fast and economical for computing resources as well as pockets.

Further, we give you an awareness session on email scams and list 10 email scams, which are most prevalent and dangerous. Beware of these scams.

We also bring you a report on US FBI's anti-crime network apart from some more highly informative reports and analysis.

I am sure, you will read, learn and enjoy.

Wishing you a Happy, Prosperous, Cyber Secure, Terror-free and Peaceful coming year – 2010.

Happy reading,

Rakesh Goyal
Editor

CONTENTS

CCC News
Issue 0013
31 December 2009

Rakesh Goyal
Editor
editor@cccnews.in

Published by
CCC Media
Mumbai, India

LAST ISSUE DOWNLOAD COUNT : 160,000+

ANALYSIS

Top Five Reasons for Security FAIL

The Internet security industry has seen every type of security solution fail. While there are exceptions, one can learn some general principles as to why things fail. Below are some observations.

The weakest link

"Security is only as good as its weakest link." This is probably the most well-known adage. Surprisingly however, many security solutions fail because of it, as the weakest link is often not obvious. This is best demonstrated with a couple of examples from the encryption world.

Take the best encryption algorithm you can find with the largest key length possible. Let's assume it is totally secure. Did you use the same level of sophistication when choosing the encryption key? If your encryption key is based on a password, for example, it is likely based on just a small number of bits and is expanded into the larger key size by the encryption software. However, it is still dependent on this small number of bits and is much weaker than you think.

Then there's the question of how you communicate that key to another party. Often times, communicating is the weakest link. A classic example is the use of One Time Pad (OTP), which has been in use since World War II. The OTP "key" is basically as long as the plain text is being encrypted, and theoretically it can be proven that OTP provides perfect security. Is that so? The weakness lies in how you communicate that OTP to the other party, and how you use it afterwards. Even if you send a messenger carrying that key to the other party and you're sure it hasn't been breached, common problems in operating such a system can render it extremely weak. If for some reason, you use some of the OTP more than once, there are simple cryptographical methods that would enable a third party to intercept and read your communications easily. The US was able to intercept communication of a Soviet spy ring by leveraging this principle.

As you can see, the weakness is often peripheral to the main part of the solution that you know or believe is solid.

Industry standard vs. proprietary

Resorting to proprietary solutions may give a small advantage due to "security by obscurity," however, it is dangerous to use solutions that are not widely scrutinized. Encryption is again a great example.

Using industry standards like AES means numerous experts have reviewed the algorithm and did not find serious issues. And if they do find them, you will know about it. Take first generation WiFi encryption (WEP). This method was very quickly shown to have serious vulnerabilities. Since it was a standard, the word quickly got out and it was replaced by stronger methods.

Be especially wary of vendors who do not expose their algorithms and make strong claims as to their strength without backing up those statements.

The right solution to the wrong problem

The problem needs to be clearly defined if security is to be effective. Otherwise, you can find yourself with a good solution that does not address your real issues.

Take the firewall, for example. While it may be a good solution for some issues, if you have a database running behind the firewall it will not block application-level attacks such as SQL injection. These are common and dangerous attacks, but most firewalls do not address them, and dedicated solutions are required.

The human factor

"If you leave it to the human factor, it will break." If you rely on the end user, and the end user is not knowledgeable enough or cannot be bothered, security is seriously lacking. A couple of examples can make this clear.

First, I find most personal firewalls useless. What good is a firewall that asks a novice user, "Do you want to allow Microsoft MAPI protocol?" What should the user say? Yes? No? If you answer wrong, either you block a vital service, or you open up for attack.

A more serious issue is that of phishing scams. These are probably the hardest to defend against. Basically, if someone can fool you into entering the password for your bank account into some fake form on the Web, or even over the phone, that's a sure recipe for identity theft. Why is this so difficult to prevent? Because it comes to the human factor. Today you have no control or knowledge of such a scam being

perpetrated, and if you only have your password for authentication that's too bad. Even if you put two-factor authentication into the bank's Web site, you still may have given valuable information such as your social security number to the wrong person.

Usability

Security must be usable in order to succeed. The best security is to cut off all connectivity, however this is extreme and not workable. So, ease of deployment and use is what makes it secure. After all, if you can't or won't use it, there's no security in place.

One example that springs to mind immediately is intrusion detection systems (IDS). While obviously important, many have forsaken them because they generate so much output and logs. So, unless you have enough bandwidth (i.e., personnel) to go over all these logs, the solution is not really effective. Similarly, many intrusion prevention (IDP) and data loss prevention (DLP) solutions generate false positives, thereby blocking authorized traffic. This is why many companies don't use them "in-line." Typically, just the basic, most obvious traffic is actually controlled "in-line," and most of the traffic is just logged to be reviewed later by an administrator. Obviously, again this is not an ideal solution.

Summary

The above are all easier said than done. Security is elusive and constantly changing. However, it is worth keeping these principles in mind when making security decisions. Define your problem well, find the weakest links, go with industry standards, minimize user involvement and keep it simple.

Courtesy : Adi Ruppin; CSO; www.computerworld.com
December 11, 2009

ANALYSIS

Compliance as Security: The Root of Insanity

There is an ever-increasing pressure for security executives to be a champion of compliance within their respective organizations. Given that there seem to be new or changing compliance requirements emerging on a fairly regular basis, this can be viewed as both a blessing and a curse.

As our government acquires increasing financial interests in some private business sectors, this trend may continue to escalate.

The blessing is that in some instances it gives the security function some additional leverage to drive results and deliver greater overall value. The curse is that the regulatory compliance requirements just add to the already voluminous amount of reactionary items that already exist on the security executive's plate. The security function is an area of responsibility that already has far too many variables that cause reactionary behavior if permitted. In some organizations this additional set of variables can be the straw that breaks the camel's back.

One of the goals of any sound information security program should be to move from a reactionary posture to a more proactive one with the institution of appropriate programs, process, procedures and controls in place. These are the building blocks of the security function and should be in place to allow the individuals responsible for the various aspects of the security function to be proactive where it is possible to do so, such as consistent processes to move forward with the latest security updates sooner rather than later. Such action is not only proactive, but reduces reactionary behavior in the future.

This is not to imply that a security program can completely reduce the need for being reactive in some instances. By reducing the areas where this reactionary capability is needed, the response to those specific areas can be more efficient and effective, allowing resources to be used for more proactive and strategic pursuits. This equates to less overall impact and a higher overall value contribution to the organization as a whole.

In order to move away from this reactionary mentality it is necessary and helpful to take a step or two back and think about how the end game of your security program needs to look.

A basis for a successful security program typically begins with one of the standard frameworks that are available, such as ISO27002 or COBIT. Some of these frameworks are more complete than others but in general these standard frameworks are not enough by themselves. Currently none of the existing regulatory or industry requirements and standards take into account the entire spectrum of controls that are needed to ensure the overall security of the enterprise.

For example, the ISO27002 specification has a section for "Business Continuity Management." While PCI provides some very prescriptive guidance around areas such as wireless, firewall placement, the use of two-factor authentication, which ISO27002 does not, it does not mention in any great detail disaster recovery and or business continuity.

In fact from one point of view to have a viable disaster recovery program can be viewed as a disadvantage from a PCI perspective. Having backup data with card holder information increases the overall scope of organizations PCI compliance unless that card holder data is rendered unreadable. At least one breach of an organization that had achieved PCI compliance was due to having certain repositories of backup data not included within the scope of the card holder data environment.

Sarbanes-Oxley Section 404 mentions very little in the areas of wireless or firewalls, but at least makes the implication around disaster recovery and business continuance capabilities by specifying some high level requirements for "Data Management." Overall, Sarbanes-Oxley Section 404 is not very prescriptive in regard to what to do or how to do it.

One thing that nearly all of the standard frameworks and the most prevalent regulatory requirements have in common is the requirement to have a security policy in place. The downside is that there is very little synergy between these frameworks and regulations regarding the content of those policies.

Approaching this from the direction of building specific solutions or groups of solutions to answer each compliance requirement will ultimatley lead to an overall security posture that is lacking basic elements and is inherently insecure. Such an approach may create a security function that is more reactionary than it was prior to having the regulatory compliance variable factored into the mix. This leads us to the undeniable realization that while a byproduct of security is compliance, the reverse couldn't be further from the truth. Given that realization, hopefully we can all be somewhat in agreement that compliance is a poor excuse for security!

Unfortunately, there are many organizations' that have only realized this after a breach has occurred. Recently an individual from Heartland payment systems was quoted as stating that "While PCI is a great beginning. It is not in and of itself enough to make you secure."

This is a positive sign that the mainstream is becoming aware of this phenomenon that compliance does not equal security.

To achieve a comprehensive security program that allows the security function to move toward and maintain status as a strategic function it must do the following with regard to compliance:

- Develop a long term plan or "road map" for information security within your organization and include provisions for the known compliance requirements;
- Work closely with your senior business executives as you create this "road map", so that they can understand where you are going, how it will affect their part of the operation, and it will give those business leaders an opportunity to provide you with better information to build it right the first time;
- Share the vision of your "road map" with your entire security organization and empower them as evangelists of that vision;
- To the extent that your are able, plan for potential future compliance requirements in your road map;
- Think of these potential new requirements as you build the various security capabilities within your organization. Try to build in the ability to adapt to new or more stringent compliance requirements without major upheavals to current processes, procedures and controls in place;

Once the 'road map" is institutionalized and you are progressing toward the defined end game the security team will become less reactionary and more proactive. Once this state is achieved and is sustainable, your security program will be providing demonstrable value to its enterprise and can truly be a strategic partner to the business.

Hopefully over time more and more organizations will come to the realization that regulatory compliance is a beginning and not an end to the ongoing process of securing the enterprise.

Courtesy : Jason Stradley; CSO; www.computerworld.com
December 8, 2009

REPORT

An introduction to the US FBI's anti-cyber crime network

The FBI explained how its anti-cyber crime task force works at a Congressional hearing this week, and outlined the Bureau's latest accomplishments, which include catching the masterminds of a coordinated raid on over 1,000 ATM machines. But nobody thinks the United States is prepared to stop a really bad attack through cyberspace on our financial or physical networks.

The Federal Bureau of Investigation told Congress this week that when it comes to cyber crime, terrorist groups like Al Qaeda aren't the sharpest pencils in the cup, but they're not out of the game either. "It is always worth remaining mindful that terrorists do not require long term, persistent network access to accomplish some or all of their goals," Steven R. Chabinsky, one of the Bureau's Cyber Division directors, explained to a Senate Judiciary Subcommittee. "Rather, a compelling act of terror in cyberspace could take advantage of a limited window of opportunity to access and then destroy portions of our networked infrastructure."

And there are lots of such windows, Chabinsky added, since, "we, as a nation, continue to deploy new technologies without having in place sufficient hardware or software assurance schemes, or sufficient security processes that extend through the entire lifecycle of our networks."

Thus the FBI has set up its own network to respond to whatever comes down the pike. Time will tell, and probably soon, how effective it is, but Chabinsky laid it out all the parts at the hearing. They include a division within the bureau, an inter-federal task force, an alliance with state, local, and industry enforcers, and a consumer complaint center.

Big news

Before unpacking these components, it should be noted that cyber crime is big news these days, with top officials repeatedly warning that the United States is not prepared for a major attack through the net on its financial or physical structures. "The architecture of the Nation’s digital infrastructure, based largely upon the Internet, is not secure or resilient," the White House concluded in its recent Cyberspace Policy Review.

Millions of Americans got a sense of the global situation on a recent 60 Minutes feature, which noted that a cyber attack probably took out the power in several cities in Brazil between 2005 and 2007. Then they learned about our "electronic Pearl Harbor," described by Jim Lewis of the Center for Strategic and International Studies:

"Some unknown foreign power, and honestly, we don't know who it is," Lewis explained to 60 Minutes' Steve Kroft, "broke into the Department of Defense, to the Department of State, the Department of Commerce, probably the Department of Energy, probably NASA. They broke into all of the high tech agencies, all of the military agencies, and downloaded terabytes of information." And last November some sleuths, possibly just by leaving thumbnail drives around, managed to get into the U.S. Central Command network (CENTCOM). Thumbnail drives are now banned from use at the agency.

That is why the White House cyberspace assessment concluded that the Federal government "is not organized to address this growing problem effectively now or in the future." And that's why we're seeing Capitol Hill hearings on the extant structure and how to improve it. Here's how the FBI is fitted to deal with the problem at this point.

Phish fries

The FBI's first line of defense against cyber crime is its Cyber Division. It has about 2,000 special agents who have received some kind of instruction in this field, and another 1,000 with more advanced training.

The Cyber Division's most noted recent accomplishment was a raid completed in October dubbed "Operation Phish Fry." The 100 people caught in this sting are accused of stealing about $1.5 million from U.S. bank account holders via phony email solicitations—complete with links to bogus bank websites. About half the defendants are Egyptian citizens who sent out the phishing messages and broke into the bank accounts. The other half hail from Nevada, California, and North Carolina. They're accused of transferring the ill-gotten money to US bank accounts, then siphoning it out of the country.

What was significant about Phish Fry was that it involved an unprecedented partnership with Egyptian police. Catching up with these kind of assaults isn't easy. It took about a year for the Cyber Division to collar the Eastern European masterminds of a massive simultaneous heist of 2,100 ATMs in 280 cities in the US, Canada, Japan, the Ukraine, and Hong Kong. The Great ATM Robbery was quite an operation, which involved penetrating a credit/debit card processing company, identifying PIN numbers, then coordinating a global network

of baddies who strolled over to ATMs and collectively helped themselves to $9 million in cash.

But the ultimate goal is stopping these virtual raiders before they strike. The FBI's Operation Dark Market seems to be the closest step towards that Holy Grail. The agency claims the so-named online network was a kind of exclusive stock exchange for crooks, where they bought and sold stolen financial data. Dark Market had 2,500 registered members. An FBI operative managed to talk his way into a job as a systems administrator for the cabal. The end result was 56 collars around the world.

Infragard

Then there's Infragard. Coordinated by the FBI, it's is a fellowship of federal, state, local, industry, and academic cybercrook catchers and watchers. Infragard has about 33,000 participants in almost 90 cities around the country, and you can apply to become a member yourself. The point is to build an accessible community for the FBI to contact on any given cyber-crime problem, especially in the private sector, where IT managers and policy folk are understandably touchy about this stuff. "No governmental entity should be involved in monitoring private communications networks as part of a cybersecurity initiative," warned Gregory T. Nojeim of the Center for Democracy and Technology, speaking before that Senate hearing.

Mindful of these concerns, Infragard hangs out around the margins between government and the private sector, "to promote ongoing timely dialogue," in the FBI's own words. Its chapters work with FBI Field Offices in the same geographic area. Infragardians conference on the latest technology and hold hacking contests.

Here's the deal, as far as we can tell. You join Infraguard and become part of the FBI's information cohort. In exchange, you get the following cool stuff:

- "Network with other companies that help maintain our national infrastructure. Quick Fact: 350 of our nation's Fortune 500 have a representative in InfraGard.
- Gain access to an FBI secure communication network complete with VPN encrypted website, webmail, listservs, message boards and much more.
- Learn time-sensitive, infrastructure related security information from government sources such as Department of Homeland Security and the FBI."

Needless to say, this makes people nervous. The Progressive magazine ran an exposé about Infragard in 2008 titled "The FBI Deputizes Business." The piece suggested that the organization may have given its members authority to "shoot to kill" in national emergencies. The FBI strongly denies this. "Patently false," FBI Cyber Division director Shawn Henry called the assertion. But it's likely that civil-liberties-minded observers will continue to squint at Infragard for the foreseeable future.

Complain complain complain

Then there's the Internet Crime Complaint Center, a collaboration between the FBI, the National White Collar Crime Center, and the Bureau of Justice Assistance (BJA). The point of IC3, as it's called, is to provide a place for victims of online theft to make complaints, a centralized system for the government to take them, and a means to learn what the bad guys are up to this week.

IC3 received almost 280,000 complaints last year and did something about over 70,000 of them. In many instances it referred them to state and local law enforcement agencies. IC3 also issues regular advisories on the latest mischief. These include alerts on the latest social networking fraud techniques, tips for SQL programmers on protecting their sites from hackers, and even warnings about e-mails pretending to be FBI warnings about Al Qaeda.

The FBI, it should be noted, is just one component of the National Cyber Investigative Joint Task Force, which it leads, and which consists of representatives from 19 government agencies that struggle with cyber crime. But it's unclear to what extent that coalition is going to have any obvious impact on the ground war against large scale roguery on the Internet. The spotlight will more likely continue to shine on the Bureau and Department of Justice's efforts in this regard—success measured by results to some, or judged by others by their impact on the nation's civil liberties.

Courtesy : Matthew Lasar; arstechnica.com
November 19, 2009

REPORT

The security nightmare formula

According to the Cisco 2009 Annual Security Report, small errors on the part of computer users or their IT departments may not wreak havoc on their own, but in combination, they dramatically increase security challenges.

Here's their recipe for the "nightmare formula" that organizations need to avoid or mitigate:

Easy-to-guess passwords and password reuse

Obvious strings of numbers , mothers' maiden names, or simply using the word "password" as a password make it easier for criminals to break into accounts and to reset passwords. Even more problematic is the reuse of the same or similar passwords, or the same answers to password recovery questions, from site to site. Read more on password best practices.

Inconsistent patching

Conficker, the big botnet of 2009, gained traction because computer users failed to download a patch that was readily available from Microsoft. Although most of today's attacks are launched via social media networks, criminals still look for ways to exploit these old-style vulnerabilities.

Getting too personal

By disclosing information, such as birth dates and hometowns, social media users make it far too easy for criminals to break into private accounts and gain control by resetting passwords. Corporate users are not immune to this trend, frequently using Twitter to discuss business projects. Read our interview with Brian Honan for an insight into social networking privacy.

Overdose of trust

Social media users are placing too much trust in the safety and privacy of their networks, responding to messages, supposedly from their connections, with malware-laden links.

Outdated virus protection

Computer users fail to update their anti-virus software or let subscriptions lapse, leaving their systems more vulnerable to attacks that might normally be easy to block. Worse, they may be running fake anti-virus software. In addition, individual users may fail to enable easily available security features built into their operating systems or web browsers, such as firewalls.

Not using available security products

Users often assume anti-virus is all they need to be "safe." Thus, they don't take advantage of simple, tried-and- true security measures, such as personal firewalls and browser security features, which can provide an extra layer of protection.

"It won't happen to me" syndrome

This is perhaps the most potent ingredient in the "nightmare formula". Users intentionally violate policies and knowingly engage in risky behavior online because they believe they won't be the victim of a cyber attack or compromise their employer's cybersecurity.

Courtesy : www.net-security.org
10 December 2009.

PREDICTIONS FOR 2010

Hot security predictions for 2010

Looking forward to 2010 while trying to erase the memory of 2009 -- here are my security predictions for the new year.

- Security funding increases by more than 10% to recover from a year of cuts. Our research shows that security is one of the areas least likely to suffer severe funding cuts. However, given escalating threats, a flat security budget in 2009 may have been a step back for companies. Expect an attempt to make up for 2009.

- Congress creates new regulatory compliance mandates. Enron gave us the Sarbanes-Oxley Act (SOX). What will 100x Enron give us? The math of compliance is shocking because it represents "assymetric warfare". A few sentences of legislation (SOX section 404?) can lead to billions in spending. The financial meltdown of 2008 to 2009 will lead to extensive and very costly regulation, in financial services and beyond.

- Self-propagating mobile phone worms and Trojans. Mobile security will get slightly worse as the proliferation of applications and smart devices broadens the attack surface. While we've seen worms on iPhone, they have not been self-propagating, depending on PCs to spread. Expect to see true self-propagating threats on iPhone and Android systems in 2010.

- Cloud computing providers introduce encryption-at-rest and other security capabilities "as a service". With security as one of the main impediments to cloud adoption, expect to see encryption, VPN, intrusion-protection systems and other security capabilities offered as a per-hour billable service. Amazon's Virtual Private Cloud is just the beginning. This could become a key area of competition in 2010.

- Security in the cloud expands with new services. In addition to cloud computing, managed security services (security in the cloud) will also expand. Expect to see data-leak prevention, encryption, directory and authentication services provided by MSSP in addition to the old staples of antispam, antimalware and firewall.

- Desktop virtualization grows. Beyond thin-client virtual desktops, companies will begin looking at on-laptop virtual machines as a way to create secure corporate desktops with easier deployment. A virtual machine can use snapshots to revert to a known-good (known-secure) configuration providing a higher degree of security for online banking or secure corporate applications. Work and play can co-exist on hardware while maintaining separation. Or you could just pretend your employees only use work PCs for work -- good luck.

- The FBI issues tens of thousands of security letters to get records on individuals without warrants. Congress investigates and is appalled at the FBI's "underreporting". The FBI promises to do better (see 2009, and 2008 and 2007....). The 4th amendment continues to erode into meaninglessness.

- Real ID dies a deserved death and is abandoned in 2010. The brain dead idea of better-security-via-universal-ID unfortunately persists despite the enormous number of identity theft victims created by over-reliance on SSN.

- The Transportation Security Administration stops wasting billions of dollars in traveller delays by confiscating water bottles and removing shoes. Instead it focuses on real threats based on rational risk assessment, not security theater based on movie-plots (hat-tip Bruce Schneier). OK, unlikely, but I can dream, can't I?

As always, I will revisit these at the end of the year and provide a critical analysis of my success rate.

Courtesy : Andreas M. Antonopoulos; www.computerworld.com
December 16, 2009

PREDICTIONS FOR 2010

Top 10 Identity Theft Predictions For 2010

I've joined forces with the Identity Theft Resource Center to expand the pool of knowledge about identity theft issues.

As nationally recognized experts in this crime, we have come up with ten predictions for what the nation can expect in the area of identity theft in 2010 and beyond.

1. **More Scams**: The recession will lead to more scams. Whenever our nation has faced a difficult time, thieves have found a way to use the problem to their advantage. In my adult life, I've never seen more variations of old scams and the degree of sophistication in newer scams.

2. **Job Scams**: Criminals will take advantage of increasing unemployment rates by tricking desperate people searching for job listings. These fake job listings and work-at-home scams will eventually end with the job seeker providing Social Security numbers to criminals. If the job description is not one that you would see printed on a business card or you are asked to front money, it's a scam.

3. **Newbie Low Tech "Desperate" Identity Theft**: Additionally, there will be an increase in the number of individuals – who have no criminal history – beginning to explore the crime of identity theft for financial gain. For these thieves, it will be about quick money. Once desperate people max out their credit limits and wreck their own credit histories; they will start to use Social Security Numbers that they can easily access.

   These new identity thieves will take advantage of low tech methods – stealing credit card numbers, dumpster diving, making phone calls, or phishing for credit card numbers. These techniques may also include placing ads in auctions and Craigslist for phantom products for sale to get either credit card numbers or cash.

4. **All-in-the-Family ID Theft**: Desperation will lead to more child identity theft and "all-in-the-family" cases, as well as the fraudulent use of numbers belonging to close friends, roommates and fellow workers. It has long been documented that a significant percentage of identity theft cases are

perpetrated by people close to the victim. We predict that this number will increase during these tough economic times.

5. **Child Identity Theft**: The ITRC has noted that nearly 10 percent of its case load, for the past six months, involved child identity theft issues. These cases often involve more varied components of identity theft than ever before. Some people have finally realized that a child's SSN can be used for more than just opening a line of credit.

6. **Medical Identity Theft**: While not a new crime, this will reflect the distress of those who have become unemployed. High COBRA premiums, growing individual medical insurance costs, or the inability to afford insurance or medical care will cause a spike in this area of identity theft. The Social Security Administration has noted an increase in uninsured people using the coverage of a friend, relative or even a stranger to get medical care.

7. **Insider Identity Theft**: In the coming year, this will increase due to the failure to follow simple security protocols in the workplace. This will create opportunities for thieves to gain access to personal identifying information retained in databases or paper files. Additionally, the lack of computer security measures and the increasing skill levels of hackers will lead to larger and more financially harmful breaches. Although a few sophisticated hackers have been arrested recently, these large, extremely damaging hacking events will continue to occur. These thieves are educating young protégées on high tech methods to access "secured" information and will likely continue to coordinate malicious attacks from their jail cells.

8. **Governmental Identity Theft**: More individuals will discover that they have become identity theft victims as they apply for government assistance and/or benefits. Not only will their own SSNs be used, but they may be temporarily denied benefits due to the use of their child's SSN, which has been used fraudulently. This type of identity theft, identified as "Governmental Identity Theft," may be associated with complications with the IRS, Social Security Administration, Departments of Motor Vehicles, Medicare and Welfare.

9. **Criminal Identity Theft**: The number of cases of criminal identity theft will continue to grow. This type of crime is defined as the use of an individual's personal information to avoid being tied to their own criminal record. In the current environment, the effects of criminal identity theft on the victims will be more apparent with the loss of employment, loss of benefits and the

increased number of arrests of victims ranging from failure to appear warrants for traffic citations all the way to felony level crimes. Criminals will continue to exploit the weaknesses of the current system and revictimize the individual whose information has been used.

10. **Social Media Identity Theft**: The meteoric rise in social media use has also created a launch pad for identity thieves. Social media identity theft happens when someone hacks an account via phishing, creates infected short URLs or creates a page using photos and the victims identifying information. My prediction for 2010 is that the increase in social networking activity, along with a user's failure to implement security and privacy settings and protocols, will lead to an increased exposure of not only the user's personal information but possibly that of their "friends."

Bottom line, there will be an increase in identity theft crimes and the number of victims over the next two years unless significant changes are made in information security. Our most important asset is our identity. And we are functioning under a completely antiquated system of identification with wide open credit and few safeguards to protect the consumer. When state governments agree with federal agencies on effective identification and industry comes together, not to profit from the problem but to solve it, only then will we prevail.

Protect your identity. Get a credit freeze. Go to ConsumersUnion.org and follow the steps for your particular state. This is an absolutely necessary tool to secure your credit. In most cases, it prevents new accounts from being opened in your name. This makes your Social Security number useless to a potential identity thief.

Invest in Intelius identity theft protection and prevention. Not all forms of identity theft protection can be prevented, but identity theft protection services can dramatically reduce your risk. (Disclosures)

Courtesy : Robert Siciliano; information-security-resources.com
December 21, 2009

PREDICTIONS FOR 2010

Top 8 Security Threats of 2010

Financial Institutions Face Risks from Organized Crime, SQL Injection and Other Major Attacks

It's a never-ending battle -- the list of naughty and downright evil security threats that challenge financial institutions and security professionals. From organized crime to SQL injection, here are the experts' choices of eight major security threats to watch in 2010.

1. Organized Crime Targeting Financial Institutions

Over the past several years, law enforcement investigations into cyber crime have uncovered global networks of organized crime groups, including overseas criminal organizations (many based in Eastern Europe) that hire and direct hackers.

Rob Lee, senior forensics investigator at Mandiant, a risk assessment firm, says the battle between "us and them" increasingly pits the financial services industry against organized crime organizations. "The days of the Maginot line of information security are long gone," Lee says, referring to the defensive World War I battle line created by Allied troops to keep German troops from invading France. The battle lines reach far wider than just an institution's firewalls, he adds.

Anton Chuvakin, an information security expert and author, predicts that 2010 will see a frightening rise in incidents attributable to organized crime. "Rampant, professional cybercrime, from the Russian Business Network (RBN) to its descendants, from individual criminal 'entrepreneurs' to emerging criminal enterprises -- all signs point to dramatic rise of cybercrime," he says. "This is simply the logical consequence of today's situation with the use of information systems: Insecure computers plus lots of money plus no punishment equals 'go do it!'"

In other words, there has not been a better time to go into a cybercrime business, Chuvakin says. "The strategy is pretty much the 'blue ocean' one, with a lot of unexplored opportunity and a low barrier to entry."

2. Assault on Authentication

The banking regulatory bodies have long called for mandatory two-factor authentication for all online banking sites. Now industry security experts warn that attacks against those traditional customer authentication methods are being challenged and defeated. Avivah Litan, a Gartner analyst, says the threats include man-in-the-browser attacks that defeat one-time-password authentication from a dedicated token (such as the popular RSA SecureID), and call-forwarding that tops phone-based authentication, as well as transaction verification using SMS or voice calls. "This is bad news for banks that use these authentication techniques to protect high-value accounts and transactions, such as those from business and private banking accounts," Litan says.

Uri Rivner, Head of New Technologies, RSA's Identity Protection and Verification division, is also seeing an increase in high-grade man-in-the-browser trojan attacks. "In 2009, the emergence of highly customizable, stealthy, MITB-capable trojan kits reached a new height with the introduction of Zeus 2.0," Rivner says. MITB trojans send money in real time, he explains, rather than just stealing credentials for sale in the underground. Rivner sees additional "Fraud-as-a-Service" models will make these kits available to more and more fraudsters. Solutions include anti-trojan detection and countermeasure services, desktop hardening, out-of-band authentication and transaction monitoring, he says.

Commercial banking has already seen early signs of man-in-the-browser attacks targeting two-factor authentication used to protect U.S. commercial online banking customers. "In 2010, we project this trend to greatly intensify, requiring commercial banks to deploy additional lines of defense such as adaptive authentication, out-of-band authentication, desktop hardening and anti-trojan countermeasure services," Rivner says.

3. More Malware

It seemed that almost every week in 2009 there was another announcement by a security researcher of a newly discovered malware variant. RSA's Rivner says malware spread like wildfire. "The rate of the malware infection of personal computers was 10 times higher during 2009 compared to 2008," he notes. Leading the infection methods are drive-by-download (taking over legitimate websites; routing visitors to an infection server) and social network infections (spamming a victim's entire social network "friend list" with links to infection servers).

Increasingly, sophisticated, distributed malware is being seen in forensic investigations of cyber crimes, says Dave Shackleford, an information security expert and SANS instructor. Criminals are also adding a flavor of social engineering to get the malware into a user's machine. "Large scale botnets are growing, and the quality of the code is improving, as these kinds of malware are increasingly funded by criminal organizations," he warns.

4. Return to Telephone-Based Fraud

One thing criminals attacking financial institutions and customers are is persistent, as seen by the number of attacks hitting US banks and credit unions in 2009. When one avenue of entry is closed, the criminals look to other ways to what they're after, says RSA's Rivner. As institutions beef up their online security, many fraudsters turned to more traditional telephony fraud.

"Armed with data stolen via trojans and phishing attacks - including 'vishing' (voice phishing), 'smishing' (SMS phishing or text phishing) and variants of spear phishing, fraudsters around the world call customer service departments at banks, credit unions and credit card companies in order to perform fraud called account takeover," Rivner says. These fraudsters often outsource the actual phone call to multi-lingual third party services provider operating 24/7 out of Russia, he adds. "Caller ID spoofing is also prevalent," he observes.

5. Increased Insider Threat

The trusted insider is the most dangerous foe for any institution -- and the most feared, as seen by the amounts of money and data taken by insiders The prevalence of insider crime can be blamed on several factors, but the insider threat at financial institutions is increasing, notes Shackleford. "I see there will be an increase in internally-driven fraud, caused in part by the bad economy and also the ease of access to data," he predicts.

Tom Wills, Security and Fraud senior analyst at Javelin Strategy and Research, agrees and adds the insider threat -- with the insider defined as anyone with access to the extended enterprise, not only employees and contractors, but partners and suppliers too -- may have financial problems that push them toward the crime. "Additionally, you have to consider individuals with significant IT knowledge who may not be fully employed and may have incentive to perform activities that they would not have previously," he notes.

Nathan Johns, a Crowe Horwath consultant, says disgruntled employees may also turn to crime. "These are people who are not receiving raises,

bonuses, or potentially being laid off, who have the opportunity to do activities that they would not have done in better times," he observes.

Johns also warns that unauthorized access by former employees can lead to problems. "There has been an increase in people being released by organizations, but often times the removal of their access rights is lagging their departure from the organization," he says.

The employees who become insider threats may do so without even knowing they're involved, warns RSA's Rivner. "Already thousands of Fortune 500, government and bank employees are infected with financial trojans that targeted them as consumers. As a side-effect, there are also thousands of infected corporate laptops or PCs used at home for remote access via a VPN," he warns.

Rivner expects 2010 will see fraudsters developing ways to monetize these infected resources, which can lead them straight into the affected organizations' networks. "Bank employees will be a primary focus for these cybercriminals," Rivner predicts.

6. Mobile Banking Attacks

The move to mobile banking by financial institutions that want to offer customers instantaneous access to their accounts is catching fire around the country, with hundreds of institutions now offering customers the ability to look up their account data and balances on cell phones. But security experts see trouble ahead when institutions begin allowing more than just account balance checks to happen. The chance for fraud via the mobile phone is already here says Ed Skoudis, lead forensic investigator for InGuardians, a security forensic firm. "Exploits against the ever-growing base of smart phones [are on the rise], leading to the possible building of a botnet based on iPhone or Android phones," Skoudis observes.

RSA's Rivner concurs with the propensity for fraud in the mobile banking sector saying, "Mobile banking fraud is coming. More customers are enrolling in mobile banking, and more services are offered via mobile channels. Banks in Asia and Europe are already experiencing mobile trojans and SMS redirection attacks." He expects the U.S. to experience the first wave of attacks towards middle of 2010. "Banks will start funding the extension of their online banking protection to the mobile channel," he predicts.

Part of the problem is that customers don't always pay attention to what they're receiving on their mobile devices, says Johns of Crowe Horwath. "People rely more and more on their BlackBerrys and smart phones, and don't pay attention to the information that they are

getting on them, and they push back to security being installed on the devices," he adds.

Javelin's Wills sees mobile fraud happening if banks start to enable full service banking on mobile devices. "This means money movement instead of just checking balances and finding ATM locations," he says.

The mobile target will continue to grow, says Shackleford, and as smart phones become more sophisticated, the number of attacks will grow too. "In many cases, these devices contain a huge amount of sensitive data, as well, and could even be a vital component of newer two-factor authentication used by banks," he says.

7. Web 2.0 and Social Media Attacks

At the same time institutions are flocking to Facebook and tweeting on Twitter, the cyber criminals are lining up their arsenals for attack via Web 2.0 and social media sites. InGuardians' Skoudis says attacks via social networking sites are the new way for criminals to get into bank accounts. "These sites are being used by the bad guys for reconnaissance to learn more about their targets," says Skoudis adding, "At the same time, they're delivering malicious content to unsuspecting users."

Institutions should also be on lookout for additional client-side spear phishing attacks will expand into new means of targeting users through use of social networks says Lee of Mandiant.

8. SQL Attacks -- More To Come

The biggest data breach on record -- Heartland Payment Systems -- was done using a "Sequel Injection," or SQL injection, attack. SQL attacks are a popular way to infect and take over websites, as seen by the recent findings by security researchers at Verizon Business. SQL injection attacks were one of the most common methods of breaching systems in the Verizon report's cases. They were used in 19 percent of the cases and accounted for 79 percent of the breached records.

There's more to watch for, says Javelin's Wills, including attacks on web applications -- especially drive-by downloads of keylogging trojans and man-in-the-middle attacks. The browser will become the favored attack vector, and zero day attacks on client-side software are also on horizon.

"Fewer operating system holes are being found, but more and more in Adobe, instant messaging, MS Office and other applications," says InGuardians' Skoudis. "The scenario would be: A victim views content

from a bad guy, and the attacker then takes over the victim's browser," he explains. This technique is used to create botnets as well as skim credit card and account information from the client machine.

He also sees infrastructure attacks, launched via an infected browser happening. "Here, the bad guy uses a compromised browser to access an enterprise infrastructure controlled by that browser including the enterprise's firewalls, anti-malware solution and possibly HVAC and related systems," Skoudis says.

Within institutions, Shackleford sees VoIP and other converged networking issues coming up "From simple denial-of-service problems to new malware that affects voice systems, this will be a growing area that affects financial institutions," he predicts.

Courtesy : Linda McGlasson; www.bankinfosecurity.com
December 21, 2009

PREDICTIONS FOR 2010

Ten 2010 IT Security Predictions

As 2009 draws to a close and a new decade dawns, CSOonline has reached out to some of the industry's best known security pros in search of insight on what the next 12 months and beyond have in store for our IT and cyber infrastructure. We started last week with Mark Weatherford, chief information security officer for the State of California, and Dan Kaminsky, network security specialist, director of pen testing at IOActive and discoverer of last year's massive DNS flaw.

We continue with predictions from Howard Schmidt, former eBay CISO and vice chairman of the President's Critical Infrastructure Protection Board, and ICSA Labs, a vendor-neutral testing and certification lab for hundreds of security companies.

1. Malware Goes Mobile

Malware for mobile devices/smartphones will escalate as more apps are provided that facilitate users ability to do more things related to e-commerce, travel and financial apps. Given that many end users feel less vulnerable on their mobile devices it could be a steep learning curve to convince them they need to take similar protections as they would on their PCs.

2. The Cloud As Security Enabler

While we have been doing some form of Cloud computing for more than 10 years 2010 will be the tipping point as to much wider adaption in all sectors. The overall net effect will give us a better chance to develop more security in the cloud using better vulnerability management/reduction, strong authentication, robust encryption and closer attention to legal jurisdictions.

3. Software Will Be Tested -- For Real

Procurement actions will require more robust testing of software and firmware to insure significant reduction of many of the vulnerabilities that we are dealing with today. This might even rise to the level of some sort of software "certification" schema to show consistency of best practices.

4. Two-factor Authentication Becomes the Rule

2010 will be the year for wider adaption of two-factor authentication for the end users. With federation of the many various types of two factor authentication that are around today we will finally see strong authentication become the rule NOT the exception.

ICSA testing and certification lab

1. PCI Compliance Continues to Drive Adoption of Web Application Firewalls (WAFs)

The WAF market is maturing. WAFs are pushing into the cloud more and more, and Gartner, Inc. is planning for the first magic quadrant on WAFs.

2. Network Attached Peripheral Security (NAPS) Threats Grow

With more network-attached devices than ever before, there are even more opportunities to cause harm. This year's uncertain economy spurred an unprecedented number of layoffs and the risk of disgruntled employees stealing confidential company information is greater than ever. Using unsecured printers and network-connected security cameras that can be manipulated, employees are able to cover their tracks when accessing restricted areas.

3. Social Networking Threats Skyrocket

As more and more businesses turn to social networking sites to extend their customer reach and build brand awareness, sensitive data becomes even more available and vulnerable. This past year, the KoobFace worm spread like wildfire through several social networks including Facebook, MySpace, Friendster and Twitter. In October, a massive bot-based attack, Bredolab, affected three-quarters of a million Facebook users by sending fake password reset messages. Vendors and purveyors of social media sites need to take a more active role in educating their users about threats like Bredolab in 2010.

4. Windows 7 Flaws Revealed

The widespread adoption of the Windows operating system naturally makes it a key target for malicious threats like viruses, bots and worms. In fact, just last week on December 8th, Microsoft issued patches for three critical bugs found in Internet Explorer 8.

5. Spam, Phishing Go Mobile

While spam comes from all over the globe, more and more of it will originate in Asia during 2010, based on our weekly anti-spam product test reports.

6. Free AV and the Rise of Scareware

While free anti-virus products are great to decrease the growing amount of malware threats out there, users need to be cautious about rogue anti-malware products -- otherwise known as "scareware" -- that organized crime rings will use to take advantage of end-users and disable their computers. Scareware reared its ugly head this year through fake advertisements (malvertising) for antivirus on The New York Times website.

Courtesy Howard Schmidt and Bill Brenner; CSO; www.csoonline.com
December 21, 2009

AWARENESS

10 email scams to watch out

If it seems like you're getting hit with more email scams than ever, you're right. Deb Shinder explains what you and your users should watch out for to avoid being duped.

Spam is one thing. It's annoying to get email messages that are nothing but blatant attempts to sell you something. But other than using up your bandwidth, they don't really cause you any harm. Email scams are quite another thing. They aren't trying to sell you something; they're trying to steal something from you, con you out of or into something, or just scare you.

Email scams have been with us since the Internet went commercial back in the early 1990s. I remember getting those Nigerian scam messages back then. And believe it or not, they're still around. But scammers have gotten more sophisticated, and some of the more recent email scams are harder to detect — unless you know what you're looking for.

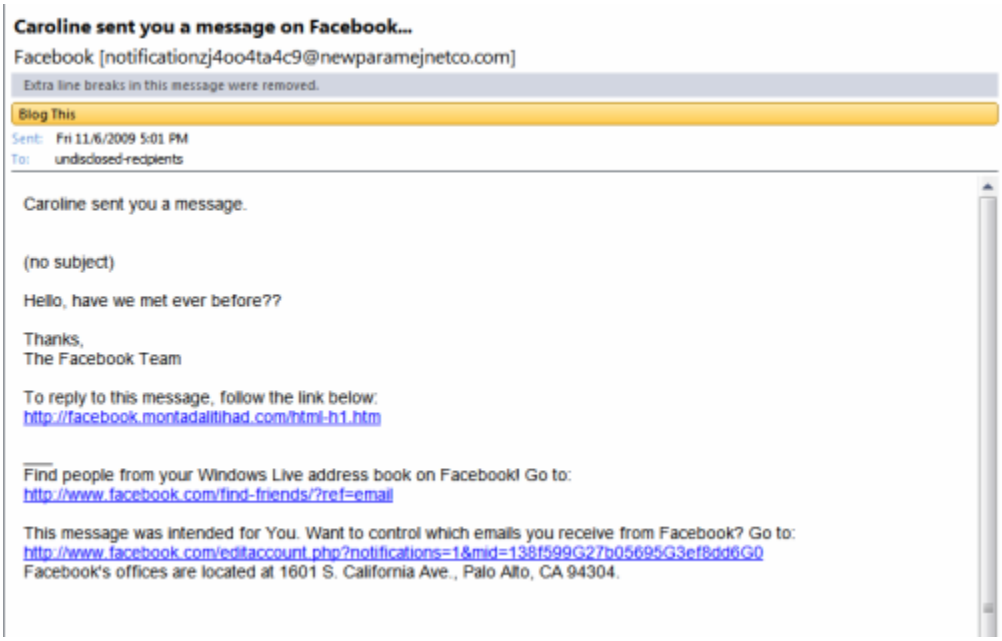
The holiday season seems to bring even more scammers out of the woodwork, perhaps because the average computer user is more vulnerable this time of the year. We're busy and in a hurry and may be less likely to notice the signs that a message isn't legit, and/or we're in a generous and giving mood and may be more likely to fall prey to a well crafted story that plays on our sympathy.

Let's look at some of the email scams that are currently going around the Internet and how you (and your users) can recognize them and keep from being victimized by them.

1: Fake Facebook "friend" messages

The popularity of social networking has surged, and scammers have jumped on that bandwagon to take advantage of the way the social sites work. For example, depending on your account settings, you may get email messages whenever someone posts to your Facebook wall or sends you a private message. Recently, I received a message with the subject line "Caroline sent you a message on Facebook." As with real Facebook messages, there was a link to click on to reply. But I get a lot of those messages, and this one didn't look quite right. Figure A shows the fake message.

Figure A



Caroline sent you a message on Facebook...

Facebook [notificationzj4oo4ta4c9@newparamejnetco.com]

Extra line breaks in this message were removed.

Blog This

Sent: Fri 11/6/2009 5:01 PM
To: undisclosed-recipients

Caroline sent you a message.

(no subject)

Hello, have we met ever before??

Thanks,
The Facebook Team

To reply to this message, follow the link below:
http://facebook.montadalitihad.com/html-h1.htm

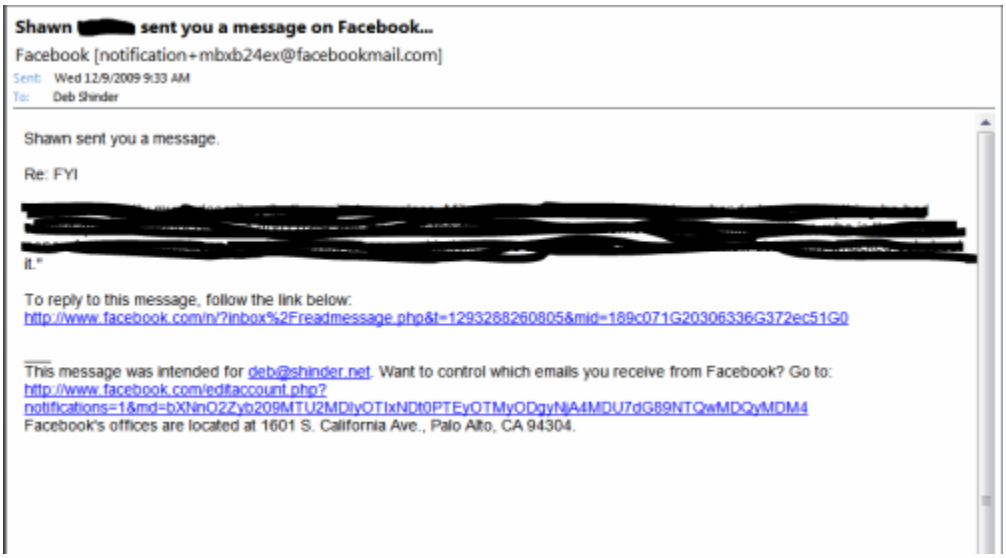
Find people from your Windows Live address book on Facebook! Go to:
http://www.facebook.com/find-friends/?ref=email

This message was intended for You. Want to control which emails you receive from Facebook? Go to:
http://www.facebook.com/editaccount.php?notifications=1&mid=138f599G27b05695G3ef8dd6G0
Facebook's offices are located at 1601 S. California Ave., Palo Alto, CA 94304.

Fake Facebook message is close, but not close enough.

I clicked back to a Facebook notification that I knew was real to compare the two. Figure B shows real message (with the content blacked out to protect the privacy of the sender).

Figure B



Shawn [redacted] sent you a message on Facebook...

Facebook [notification+mbxb24ex@facebookmail.com]

Sent: Wed 12/9/2009 9:33 AM
To: Deb Shinder

Shawn sent you a message.

Re: FYI

[redacted]

it."

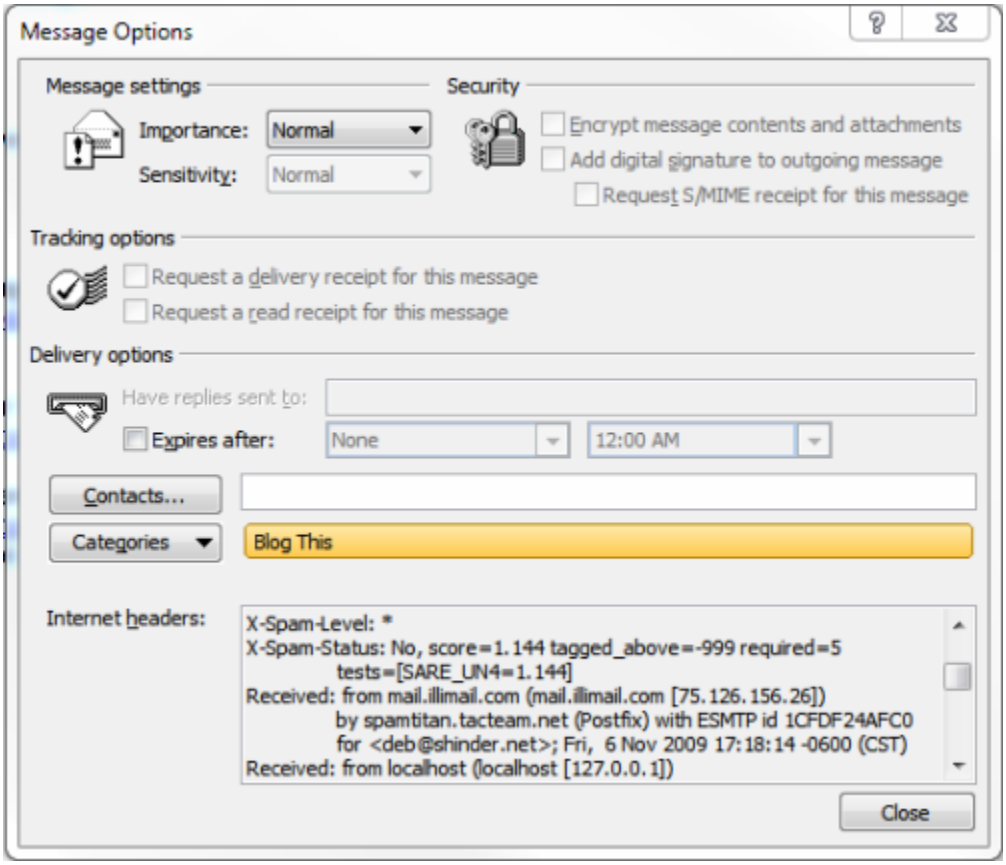
To reply to this message, follow the link below:
http://www.facebook.com/n/?inbox%2Freadmessage.php&t=1293268260805&mid=189c071G20306336G372ec51G0

This message was intended for deb@shinder.net. Want to control which emails you receive from Facebook? Go to:
http://www.facebook.com/editaccount.php?
notifications=1&md=bXNnO2Zyb209MTU2MDIyOTIxNDt0PTEyOTMyODgyNjA4MDU7dG89NTQwMDQyMDM4
Facebook's offices are located at 1601 S. California Ave., Palo Alto, CA 94304.

The real Facebook message has subtle differences.

The first thing that caught my attention was the Reply To address. I expected the URL domain to be www.facebook.com, but the one in the fake message was facebook.montadalitihad.com. If you know how domain naming works, you know that means "facebook" is just the name of a Web server in the montadalitihad domain. As if that weren't enough, I also noticed that the To field in the message didn't show my name; instead it said "Undisclosed recipients," indicating this message was sent to multiple people. All this was enough to cause me to check out the message headers (in Outlook 2007, you do this by clicking the Options icon. Figure C shows the headers.

Figure C



The Internet headers show that this message did not come from Facebook.

In a real Facebook message, the Received: field in the header would be from mx-out.facebook.com. In this one, it's mail.illimail.com. Now I knew for sure that it didn't come from Facebook.

I had opened the message in a virtual machine, so if there was malicious code attached, it wouldn't affect my real OS. Now I clicked

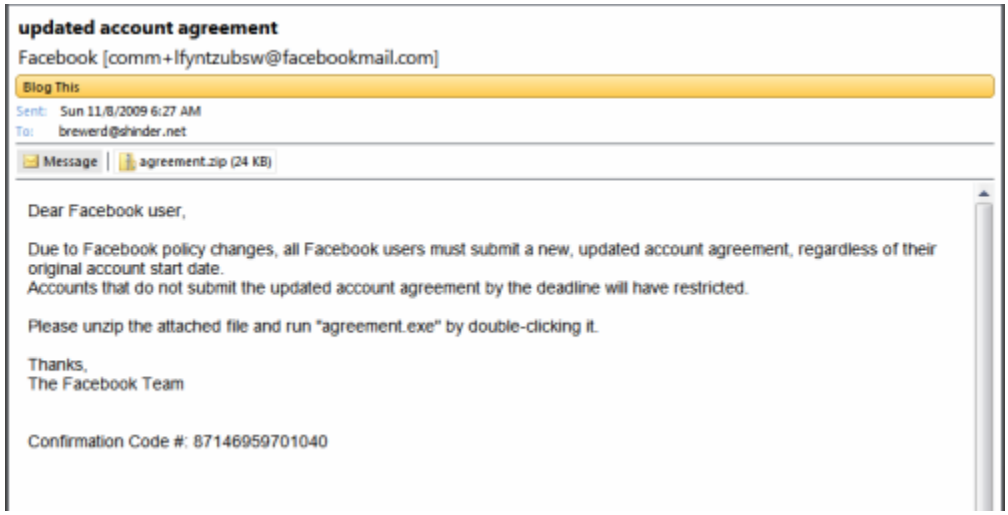
the Reply To link and found that it opened a page that looks very much like the Facebook login page. The red flag here was that I was already logged into Facebook with that Web browser. You should not get the login page if you're already logged into the service. I did not, of course, enter my credentials. That's the scam. If you do, the scammer will now have your Facebook user account and password and can hijack your Facebook site.

Of course, variations on this scam may use other popular social networks, such as MySpace or LinkedIn. If you're in doubt about the legitimacy of any "friend" message, just log in to your social network account via your browser (not by clicking the link in the email) and check your Inbox. If the message is real, there will be a copy of it there.

2: Fake admin messages

You might just ignore a "friend" message (especially from a friend you've never heard of). But scammers know that a message from the site administrator is more likely to get your attention. This message pretends to be from "The Facebook Team" and purports to notify you of a policy change that requires you to submit a new account agreement. They try to scare you by warning that your account might be closed down or restricted if you don't do it. Figure D shows this message.

Figure D



Scammers up the ante by sending fake administrative messages.

This time, the scammer did a better job with the From name, which shows to be from facebookmail.com, just like a real Facebook message. But the first clue that it's a scam is the To address. That's not my name, and that's not the name of anybody in my domain. I have our Exchange server set up to forward messages to me when they're sent to nonexistent addresses (assuming they don't meet other spam criteria, which would block them at the server's spam filters). Spammers and scammers often get hold of an email domain name and send messages to random names at that domain in hopes they'll hit on a real one.

The second warning signal is the attachment. Facebook agreements don't come as attachments; if this were real, it would direct me to a web page where I could read the new terms and click Agree. Attachments from strangers should always put you on alert.

I copied the attachment into a virtual machine and ran a virus scan on it. Sure enough, it was infected with a virus called VirTool:Win32/VBInject.gen!CN. Luckily, most antivirus programs that are up to date will be able to detect it. A check of the Internet headers on this message indicated that the Reply To address is somewhere in Germany.

3: Fear-mongering messages

While we think of scam messages as those by which the scammer profits, some don't benefit the scammer at all — except for whatever gratification a person gets from causing others to be upset or afraid. Unfortunately, this makes some individuals feel powerful.

There are many examples of these types of messages, and they usually seem to play on the current headlines. A few years ago, there was a flood of such messages warning that if you saw another car on the road at night with headlights off and blinked yours to signal to the driver, you were in dire danger of being shot as part of a gang initiation. This article details the history of this email hoax.

Similar fear-mongering scams have warned about a serial killer who lured women out of their homes by playing a recording of a crying baby and a rapist who would approach women in parking lots claiming to have picked up a five dollar bill the woman dropped.

The latest in fear-mongering messages like to play on health fears caused by all the recent media attention to swine flu (H1N1). An email message has been going around the Internet for several months warning that "The CDC says H1N1 is wiping out entire villages in Asia and expect it to hit the U.S. in January, where it will kill 6 out of 10

people." The message goes on to predict that martial law will be declared and you'll be shot if you leave your house to buy food, and urges recipients to stock up now and to buy face masks, use Purell, and take Enzacta products to "keep your immune system strong." If you weren't already a little suspicious, you probably will be by the time you get to the end, where the sender says the pandemic was predicted years ago by a Russian mathematician and that it was caused by a tsunami. Here's the full text of the message.

They always say that if something seems too good to be true, it probably is. The same goes for over-the-top bad news — especially if you're hearing it for the first time in an email message. You can bet that if the CDC had really put out such an announcement, it would be all over the mainstream news outlets.

4: Account cancellation scams

It seems that around the holidays, more of these than usual start popping up. I've received a number of messages telling me that my account has been or is about to be cancelled — purportedly from Amazon, PayPal, even from the bank. Close examination of the messages show them all to be bogus. Of course, in many cases, I already knew that, because I don't even have an account with the organization.

Here's another clue: The message contains a link that looks legit, such as www.mybank.com, but when you hover your mouse pointer over it to show the actual URL, it's something different, often with a foreign country code such as .ru (Russian) or .cn (China).

Still another clue is that these scam messages often contain typos or grammatical errors you wouldn't expect from a legitimate company.

5: Bogus holiday cards

There are numerous Web sites through which you can send virtual holiday cards to your friends, and many people take advantage of this quick and easy — and inexpensive (no postage stamps required!) — way to send season's greetings at this time of the year.

Scammers have co-opted the idea, though. They know that many computer users won't think twice about clicking a link to view a card from a friend, so they send out messages notifying you that you've received a card, with a link to a Web site that will download malicious software to your computer if you aren't properly protected.

So how do you tell the real card services from the scams? For one thing, when a friend sends you a card from a real service, it will almost always tell you the name of the sender. Scam messages are more likely to use the generic "A friend sent you a greeting." The safest way to check is to do a Web search for the card service and read about it to find out if it's a legitimate one. Or to really be safe, just ignore the card notification and send holiday greetings to your friends the old fashioned way (through the postal service) or by personal email, instead of using a Web service.

6: Phantom packages

Any other time of the year, you might be suspicious if you were notified that you had an unexpected delivery from DHL, FedEx, or UPS. During the holidays, it's a common occurrence. Scammers know this, so they're seizing the opportunity and sending email messages telling you that you have a package that couldn't be delivered because of some problem with the shipping address.

This particular scam contains an attachment that's supposed to be a form you need to print and fill out so you can pick up the package. However, there is no package and when you open the attachment, it infects your computer with a virus.

Also beware of variations on this theme. Many people know not to download email attachments, but they'll readily click a link to go to a Web site. So more sophisticated scammers will send you to a site that looks like that of the delivery service, but that delivers only malware — straight to your system.

7: Threats from the government

A sharply divided partisan political system has resulted in a growing distrust of government in many circles. Some scammers are now playing on those sentiments. A recent scam email has been going around that purports to warn you that the Department of Homeland Security and the FBI have been informed that you're allegedly involved in money laundering and/or terrorist activities. The email goes on to say that you can avoid prosecution by obtaining a certificate from the Economic Financial Crimes Commission Chairman — for only $370. Who wouldn't jump at that deal?

Many similar scams use the names of government agencies. Of course, they're all hoaxes. If you were really the target of a DHS or FBI investigation, you wouldn't be able to buy your way out of it for a few hundred bucks. And those agencies would be contacting you in person, not sending threatening email messages.

8: Census survey says…

Another recent email scam also involves the federal government, but instead of accusing you of a crime, it uses your knowledge of real, routine government activities against you. Everyone knows that the U.S. government conducts a census every 10 years, and 2010 is the year. Citizens are required by law to answer the census-takers' questions. Most people also know that many government-related tasks can now be done online.

Scammers are taking advantage of this to send phishing emails that claim to be from the Census Bureau, making it "convenient and easy" for you to fulfill your census obligation, either by filling out an attached form and emailing it back or by visiting a Web site to fill in a form. The form asks for all sorts of personal information, including the social security number and date of birth of everyone in your household, which can be used for identity theft.

In addition to asking you these personal questions, the emails may include attachments containing malicious code that can infect your computer. The same goes for the Web links contained in the email message. The Census Bureau does, in fact, send email regarding your participation in a survey — but it does not ask for detailed personal information.

9: In Microsoft (or Apple or Dell or HP) we trust

There are dozens of email scams out there that attempt to exploit users' trust in the vendors that make their computer software or hardware. These messages say they're from the vendor and range from fake security warnings with attachments that claim to be vulnerability fixes (but are really malware) to bogus "special offers" to "payment requests" that require you to download and install a "transaction inspector module" (which is really a Trojan) if you want to decline to have the payment charged to your credit card.

10: You're a winner!

There are many new twists on an old theme: You're a winner in the lottery, contest, or drawing. All you have to do to claim your prize is fill out a form and email it back. Of course, the entity awarding the prize needs your social security number because the value of the prize must be reported to the IRS.

The bad thing about this scam is that you will indeed have to provide such information to claim a prize in a legitimate contest. As a Microsoft

Windows 7 Launch Party host, I was automatically entered in a contest to win a Dell laptop — and I won. When I got the email notification, you can bet I was suspicious. Before doing anything, I checked it out with my contacts at Microsoft. Even after confirming that the notice was real, I declined to send my personal information back via email; I printed out the form and sent it via snail mail (registered and certified) instead.

Even if you really did enter the contest that you're being told you won, don't get careless. Check into the legitimacy of an email notification of the good news. And I recommend never sending your social security number or other sensitive information in unencrypted email. A legitimate contest will almost always have alternatives methods by which you can submit your information.

Courtesy : Debra Littlejohn Shinder; blogs.techrepublic.com.com
December 19th, 2009

This edition of the magazine is brought to you courtesy

Sysman Computers Private Limited

Sysman is

1. Pioneer in IT Security in India since 1991
2. Empanelled with CERT-In
3. Done over 2000 IT Security assignments
4. Provide Research Support
5. Create Public Awareness
6. Published 6 Books / 50 papers
7. An associate consultant to BSI to implement ISO 27001-ISMS

Contact –

Sysman Computers Private Limited, Mumbai

sysman@sysman.in

+91-99672-48000
+91-99672-47000

www.sysman.in