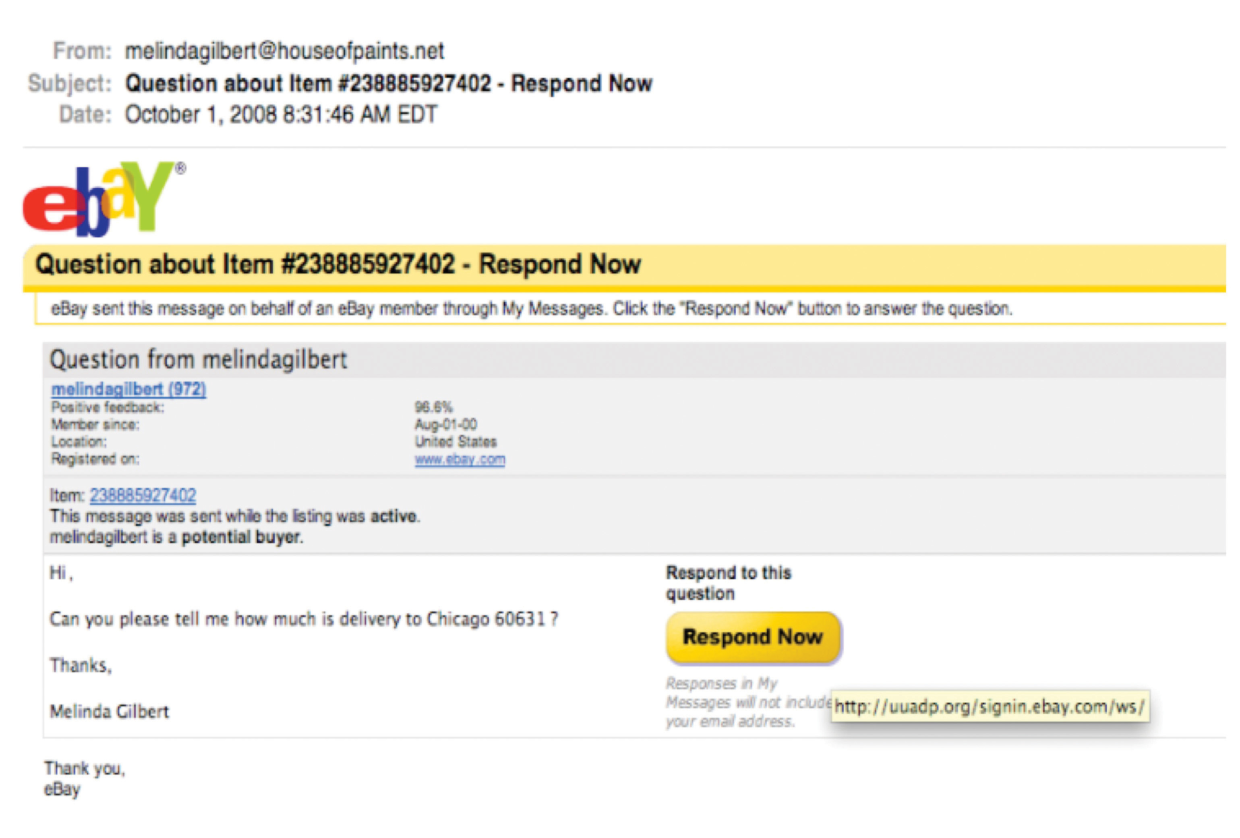
**More Notes on Security**

**More on Phishing**

This image is from a phishing scheme masquerading as an eBay message. The real destination is a compromised .org domain unassociated with eBay, but the phishers have created a directory at this domain named “signin.ebay.com” in hopes that users will focus on that part of the URL and not recognize they’re really headed to a non-eBay site.

**Web 2.0: The Rising Security Threat**

Social networks and other Web 2.0 tools are a potential gold mine for crooks seeking to pull off phishing scams. Malware can send messages that seem to come from trusted “friends.” Messages such as status updates and tweets are short, and with limited background information, there are fewer contexts to question a post’s validity. Many users leverage bit.ly or other URL-shortening services that don’t reveal the Web site they link to in their URL, making it easier to hide a malicious link. Criminals have also been using a variety of techniques to spread malware across sites or otherwise make them difficult to track and catch.

The technical openness of many Web 2.0 efforts can also create problems if schemes aren’t implemented properly. For example, Mark Zuckerberg’s Facebook page fell victim to hackers who used a hole in a Facebook API that allowed unauthorized status update posts to public Facebook fan pages. APIs can allow firms to share services, collaborate, and enable mash-ups, but if code is poorly implemented it can also be an open back door where the bad guys can sneak in.

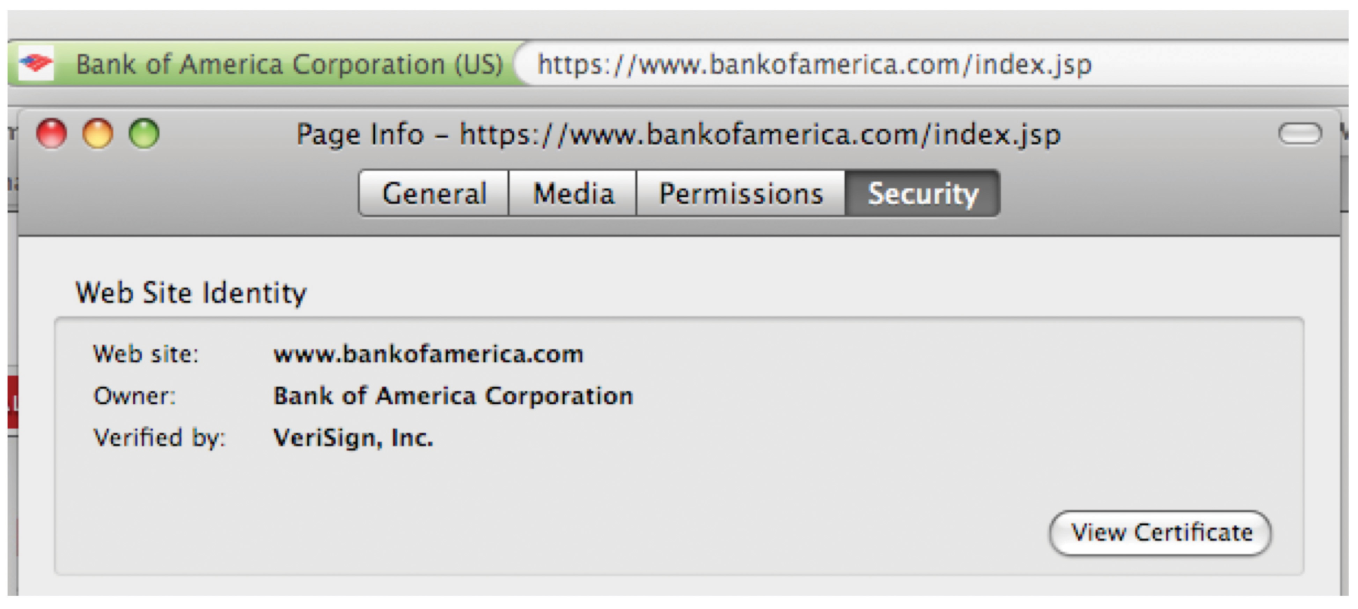
Some botnets have even used Twitter to communicate by sending out coded tweets to instruct compromised machines (zombies).Social media can also be a megaphone for loose lips, enabling a careless user to broadcast proprietary information to the public domain. A 2009 Congressional delegation to Iraq was supposed to have been secret. But Rep. Peter Hoekstra tweeted his final arrival into Baghdad for all to see, apparently unable to contain his excitement at receiving BlackBerry service in Iraq. Hoekstra tweeted, “Just landed in Baghdad. I believe it may be first time I’ve had bb service in Iraq. 11th trip here.” At the time, Hoekstra was a ranking member of the House Intelligence Committee!

**Botnets or zombie networks**. Hordes of surreptitiously infected computers linked and controlled remotely by a central command. Botnets are used in crimes where controlling many difficult-to-identify PCs is useful, such as when perpetrating click fraud, sending spam, registering accounts that use CAPTCHAs (those scrambled character images meant to thwart things like automated account setup or ticket buying), executing “dictionary” password cracking attempts, or launching denial-of-service attacks (DDoS).

**How Do Web Sites Encrypt Transmissions?**

Most Web sites that deal with financial transactions (e.g., banks, online stores) secure transmissions using a method called **public key encryption**. The system works with two keys—a public key and a private key. The public key can “lock” or encrypt data, but it can’t unlock it: that can only be performed by the private key. So a Web site that wants you to transmit secure information will send you a public key—you use this to lock the data, and no one that intercepts that transmission can break in unless they’ve got the private key. If the Web site does its job, it will keep the private key out of reach of all potentially prying eyes

Wondering if a Web site’s transmissions are encrypted? Look at the Web address. If it begins with **“https”** instead of “http”, it should be secure. Also, look for the **padlock icon in the corner of your Web browser** to be closed (locked). Finally, you can **double click the padlock to bring up a verification** of the Web site’s identity (verified by a trusted third party firm, known as a certificate authority). If this matches your URL and indicates the firm you’re doing business with, then you can be pretty sure verified encryption is being used by the firm that you intend to do business with.



In this screenshot, a Firefox browser is visiting Bank of America. The padlock icon was clicked to bring up digital certificate information. Note how the Web site’s name matches the URL. The verifying certificate authority is the firm VeriSign.

**Taking Action as an Organization  
Security Education, Audit, and Enforcement**

Security is as much about people, process, and policy, as it is about technology.

For a lesson in how important education is, look no further than the head of the CIA. Former U.S. Director of Intelligence John Deutch engaged in shockingly loose behavior with digital secrets, including keeping a daily journal of classified information—some 1,000+ pages—on memory cards he’d transport in his shirt pocket. He also downloaded and stored Pentagon information, including details of covert operations, at home on computers that his family used for routine Internet access.

Employees need to know a firm’s policies, be regularly trained, and understand that they will face strict penalties if they fail to meet their obligations. Policies without eyes (audit) and teeth (enforcement) won’t be taken seriously. Audits include real-time monitoring of usage (e.g., who’s accessing what, from where, how, and why; sound the alarm if an anomaly is detected), announced audits, and surprise spot checks.

**What Needs to Be Protected and How Much Is Enough?**

A worldwide study by PricewaterhouseCoopers and Chief Security Officer magazine revealed that most firms don’t even know what they need to protect. Only 33 percent of executives responded that their organizations kept accurate inventory of the locations and jurisdictions where data was stored, and only 24 percent kept inventory of all third parties using their customer data. What this means is that most firms don’t even have an accurate read on where their valuables are kept, let alone how to protect them.

Information security should start with an inventory-style auditing and risk assessment. Technologies map back to specific business risks. What do we need to protect? What are we afraid might happen? And how do we protect it? Security is an economic problem, involving attack likelihood, costs, and prevention benefits. These are complex trade-offs that must consider losses from theft or resources, systems damage, data loss, disclosure of proprietary information, recovery, downtime, stock price declines, legal fees, government and compliance penalties, and intangibles such as damaged firm reputation, loss of customer and partner confidence, industry damage, promotion of adversary, and encouragement of future attacks.

While many firms skimp on security, firms also don’t want to misspend, targeting exploits that aren’t likely, while underinvesting in easily prevented methods to thwart common infiltration techniques

#### Technology’s Role

An organization’s approach will often leverage multiple layers of protection and incorporate a wide variety of protective measures.

**Patch**. Firms must be especially vigilant to pay attention to security bulletins and install software updates that plug existing holes, (often referred to as patches). Firms that don’t plug known problems will be vulnerable to trivial and automated attacks. With operating systems automating security update installations, hackers have moved on to application targets. But a major study recently found that organizations took at least twice as long to patch application vulnerabilities as they take to patch operating system holes. Remember, software isn’t limited to conventional PCs and servers. Malware has infected everything from unprotected ATM machinesto restaurant point-of-sale systems to fighter plane navigation systems.

**Lock down the network.** Network monitoring is a critical part of security, and a host of technical tools can help.

Firms employ **firewalls** to examine traffic as it enters and leaves the network, potentially blocking certain types of access, while permitting approved communication. **Intrusion** **detection** systems specifically look for unauthorized behavior, sounding the alarm and potentially taking action if something seems amiss. Some firms deploy **honeypots**—bogus offerings meant to distract attackers. If attackers take honeypot bait, firms may gain an opportunity to recognize the hacker’s exploits, identify the IP address of intrusion, and take action to block further attacks and alert authorities.

Many technical solutions, ranging from network monitoring and response to e-mail screening, are migrating to “the cloud.” This can be a good thing—if network monitoring software immediately shares news of a certain type of attack, defenses might be pushed out to all clients of a firm (the more users, the “smarter” the system can potentially become—again we see the power of network effects in action).Many technical solutions, ranging from network monitoring and response to e-mail screening, are migrating to “the cloud.” This can be a good thing—if network monitoring software immediately shares news of a certain type of attack, defenses might be pushed out to all clients of a firm (the more users, the “smarter” the system can potentially become—again we see the power of network effects in action).

**Lock down partners**. Insist partner firms are compliant, and audit them to ensure this is the case. This includes technology providers and contract firms, as well as value chain participants such as suppliers and distributors. Anyone who touches your network is a potential point of weakness. Many firms will build security expectations and commitments into performance guarantees known as **service level agreements (SLAs).**

**Access controls** can also compartmentalize data access on a need-to-know basis. Such tools can not only enforce access privileges, they can help create and monitor audit trails to help verify that systems are not being accessed by the unauthorized, or in suspicious ways.

**Email** - Most corporations have strict policies on how long e-mails will be kept on their systems. Usually the period of time is about 60 days.

**Audit** **trails** are used for deterring, identifying, and investigating these cases. Recording, monitoring, and auditing access allows firms to hunt for patterns of abuse. Logs can detail who, when, and from where assets are accessed. Giveaways of nefarious activity may include access from unfamiliar IP addresses, from nonstandard times, accesses that occur at higher than usual volumes, and so on. Automated alerts can put an account on hold or call in a response team for further observation of the anomaly.

**Multiple administrators should jointly control key** **systems**. Major configuration changes might require approval of multiple staffers, as well as the automatic notification of concerned personnel. And firms should employ a recovery mechanism to regain control in the event that key administrators are incapacitated or uncooperative.

**Have failure and recovery plans**. While firms work to prevent infiltration attempts, they should also have provisions in place that plan for the worst. If a compromise has taken place, what needs to be done? Do stolen assets need to be devalued (e.g., accounts terminated, new accounts issued)? What should be done to notify customers and partners, educate them, and advise them through any necessary responses? Who should work with law enforcement and with the media? **Do off-site backups or redundant systems need to be activated?** Can systems be reliably restored without risking further damage?