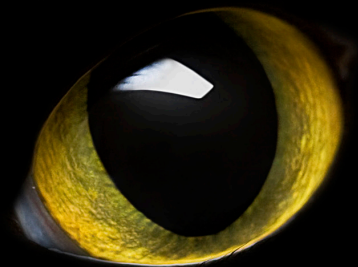
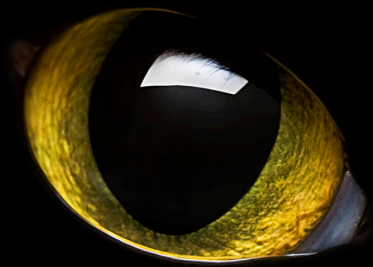


## Security threat report **2011**



cute and furry?  
or  
ruthless and deadly?

# Sophos security threat report **2011**



We will remember 2010 as a year in which our interaction with technology—and with each other—evolved because of the widespread adoption of social media and the use of innovative mobile computing devices.

We are dependent on smart devices—just ask anyone who has lost their iPhone or BlackBerry. And whether you're using a mobile device or a laptop or desktop computer, you're likely to use social networks more than ever. This new technology changes the way we communicate with our friends, colleagues and customers. This not only revolutionizes the way we live our lives, but also blurs the lines that define the way we run our businesses and use and share information.

Today, users are the content. Driving the growth, and at the same time being driven by it, the explosion in mobile computing is expanding the impact of the social web. And, the way that content is shared and accessed is now the core of a new global culture, affecting and combining the spheres of personal and business life.

Of course, this evolution of technology is closely tracked by the “bad guys” willing to exploit weaknesses in our technologies and in human nature. Cybercriminals prey on our curiosity, and perhaps our vulnerability and gullibility, and use psychological traps to profit from unsuspecting technology users. Malware scams and exploits targeting social networking websites, applications, devices, and users proliferate. At the same time, traditional attacks continue to become more sophisticated to target the most advanced software, hardware and websites.

*By preying on our curiosity, cybercriminals are able to use psychological traps to profit from unsuspecting users of technology.*



By the end of 2010, [WikiLeaks](#), a whistle-blowing website, caused a global furor. The site publishes private, secret and classified media submissions from anonymous news sources and news leaks, and led to sustained and sophisticated tit-for-tat cyber-attacks. This underlines the importance of data security and cyber-caution for large-scale business , for government and at the personal level as well.

As always, we continue to track—and where possible, thwart—the latest attack techniques and maintain protection against them. To stay secure in 2011 and beyond, it's vital that we understand how threats worked in 2010. This report identifies the threats, the way they work, and provides insight into the tools and techniques available to protect your systems and data.

# Identifying the threats: where to watch

95,000—that's the number of malware pieces analyzed by SophosLabs every day in 2010, nearly doubling the number of malware pieces we tracked in 2009. This accounts for one unique file every 0.9 seconds, 24 hours per day, each day of the year. It's a clear sign that the malware threat continues to grow at an alarming rate.

Today, more than ever before, hackers aren't just producing malware for notoriety—they're producing it for large financial gain. We track these methods of attack and constantly learn from them so we can block and protect your systems. Here's a look at the more significant threats of 2010. It's wise to keep watching these threats, as they're likely to surface again in 2011.



# Fake anti-virus software

One of the more persistent threats of the year was fake anti-virus, also commonly known as “scareware” or “rogueware.” In this widespread practice, software is inveigled into a victim’s computer system, closely resembling—and in some cases [directly impersonating—genuine security solutions](#). The user receives a warning that their system is infected with some nasty malware and forced to pay for a “full” version of the software to remove the threat. Of course, paying money to the bad guys doesn’t provide any protection. In most cases there’s no real danger, and in many cases they’re actually installing additional malware on the system and taking your credit card information. With this kind of data handed over so freely, cybercrooks can drain your bank account or completely take over your identity.

Clearly the scam is successful for those propagating these rogue products; [over half a million fake anti-virus software variants have been encountered](#). Along with the fear/response trick of the scam itself, numerous methods are used to get malicious software onto victims’ machines. Some are direct methods such as warning pop-ups activated by visiting malicious or compromised webpages, and others methods span to more generic social engineering techniques used to convince recipients of spammed emails to open malicious attachments.

A good first step to combat the fake anti-virus threat is user education, but even informed attempts to fight back are often hindered by unwise activities from legitimate sites and service providers. For example, a genuine campaign run by U.S. Internet Service Provider, Comcast, warned users of suspected botnet infections. However, this real alert was hard for some to distinguish from a [fake anti-virus software alert](#).

*cybercrooks  
can drain your  
bank account  
or completely  
take over  
your identity*

# Attacks using Internet marketing techniques

While older approaches such as email remain a threat, fake anti-virus and other malware are largely spread through the web. The search engine is our gateway to the web, and cybercrooks are skilled at manipulating search results from the engines such as Google, Bing and Yahoo! to lure victims to their malicious pages. These pages host security risks and browser exploits just waiting to infect users who are directed to these sites. There's also the [abuse of legitimate search engine optimization \(SEO\) techniques](#). Legitimate Search Engine Optimization (SEO) techniques are regularly used as marketing tools, but when SEO is abused by the bad guys, and supplemented by more devious methods, it's known as Black Hat SEO.

With Black Hat SEO attacks—known as “SEO poisoning”—search engine results are poisoned to drive user traffic to the rogue site. [Google reported that up to 1.3% of their search results are infected](#). So, with SEO poisoning, you're directed to a bad page through a poisoned search. Once a victim is lured to the desired webpage, they're redirected to these rogue or poisoned sites. On these sites, cybercriminals infect users' machines with malware or push fake goods and service to users while attempting to steal personal information.

To maximize the number of victims, crooks hijack search terms likely to generate a lot of traffic, such as rapidly breaking news stories and popular “trending” searches. In 2010, topics abused to target searchers included natural disasters such as earthquakes and tsunamis, entertainment stories such as the Oscars, the love lives of Hollywood stars and royalty, and the tragic stories of victims of cyber-bullying. [Criminals even hijacked legitimate anti-virus companies' press releases](#) as a tactic to get users to click on poisoned search results.

## Black hat SEO and SEO poisoning attacks explained

**SEO** stands for *search engine optimization*, a standard Internet marketing technique used by many legitimate firms to help promote their Internet presence

**SEO** involves careful selection of keywords and topics to increase a page's popularity and rating in search engine results, which are sorted based on link rankings

**Cybercriminals use SEO techniques** to latch onto trending or popular topics, such as major news events or holidays

**Malicious sites** reference trending search terms and are optimized to pull traffic from search engines

**Custom tools** are for sale on underground cybercriminal forums that steal content from legitimate webpages about the subject matter, and interlink pages across domains for a higher ranking in search engines

**Page visitors** are subjected to malware attacks targeting browser vulnerabilities, scareware scams and more

## What is social engineering?

Social engineering is a catch-all term for psychological tricks used to persuade people to undermine their own online security. This can include opening an email attachment, clicking a button, following a link, or filling in a form with sensitive personal information. All sorts of scams, and many methods used to spread malware, make use of social engineering techniques, and target human desires and fears—as well as just plain curiosity—to get past the caution we should all be exercising when online.

"Trojan Horse" malware is a classic example of a social engineering technique. Taking its name from the ancient tale of the huge wooden horse that the Greeks constructed and left at the gates of Troy as a gift, today's Trojan Horse also works by bypassing security defenses. This malware routinely uses the Trojan Horse scheme by disguising files as "free" or cracked software, and can include sex videos or anything other hidden means to get past security.

## Social engineering techniques on social networks

By mid-2010, Facebook recorded half a billion active users, making it not only the largest social networking site, but also one of the most popular destinations on the web. People use the Internet differently because of social networking. Young people are less likely to use email, and more apt to communicate through Facebook, Twitter or other social sites. Unsurprisingly, scammers and malware purveyors targeted this massive and committed user base, with diverse and steadily growing of attacks throughout 2010.

One of the more common types of attack hitting Facebook users is "[clickjacking](#)," also called "UI redressing." These attacks use maliciously created pages where the true function of a button is concealed beneath an opaque layer showing something entirely different. Often sharing or "liking" the content in question sends the attack out to contacts through newsfeeds and status updates, propagating the scam.

[Clickjacking](#) uses the standard arsenal of [social engineering techniques](#) to lure new victims and trick them into clicking on the disguised links, many of which developed a rather dark tone in 2010. Alongside the usual barrage of lures such as humor, [compromising pictures of celebrities](#) and major news and entertainment events, we saw a rise in increasingly bizarre and often gruesome content. [Stories of suicide](#), car crashes and [shark attacks](#), the allegedly "horrific" effects of a popular drink and over-the-top revenge stories were all clickjacking scams in 2010. On some days last year, [cybercrooks](#) introduced dozens of new scams.

Clickjacking attacks not only spread social networking link-spam, they also regularly carry out other actions such as granting access to valuable personal information and even making purchases. One of the main financial motivations behind clickjacking is money earned from survey scams.

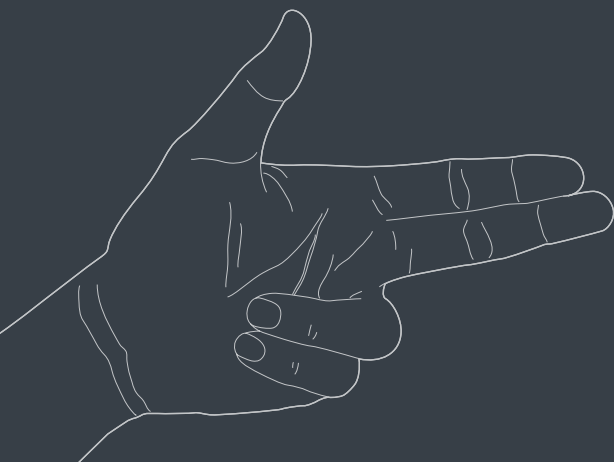
# How to avoid being fooled by social engineering techniques

1. Remember that if something sounds too good to be true, it probably is.
2. Ask yourself—why would you be singled out for a windfall or other special treatment out of the millions of other Internet users. If you can't find a good reason, it's probably a scam.
3. Don't believe everything you read. Just because an email or website is presented attractively doesn't mean that it's telling you the truth.
4. Be patient. Too many users end up the victims of Internet crime because they do not stop to think, but instead act on impulse clicking on a “sexy” link or an interesting looking attachment without thinking of the possible consequences.
5. Unless you're certain of a person's identity and authority to request such information, never provide your personal information or information about your company/organization.
6. Don't reveal personal and financial information in email. Be wary of emails that ask you to follow a link to enter such information.
7. If you think an email may not be legitimate, attempt to verify it by contacting the company or organization directly. But don't use the contact information provided in the email to make contact, it could be bogus; look up the organization's contact information yourself.
8. Double-check the URLs of websites you visit. Some phishing websites look identical to the actual site, but the URL may be subtly different.
9. Be cautious about sending sensitive information over the Internet if you're not confident about the security of the website.
10. Be suspicious of unsolicited phone calls and emails that ask for information about your employees or other information. It could be a scammer calling.

The “[Survey scam](#)” tricks users into installing an application from a spammed link. To access the application's alleged (but often non-existent) functionality, users must grant access to their personal data. This sends out links to a new stash of contacts; that also must fill in a survey form, which earns the application creators money through affiliate systems.

Facebook founders and operators insist that keeping users safe from spam and scams is a top priority, and they use large teams of security experts to remove suspect applications as soon as they're detected or pointed out by users. Yet, the problem continues to grow as the site's growing user base makes it an ever richer target for the bad guys.

The scale of malicious activity on Facebook appears to be out of control, and people are taking notice. [A Sophos Poll in June 2010](#) found that 95% of respondents wanted Facebook to do more to [prevent “likejacking” attacks](#), (essentially clickjacking by liking something on Facebook) and urged the site impose stricter controls on the plugin. The social media site, however, is either unable or unwilling to invest the necessary resources to stamp it out.

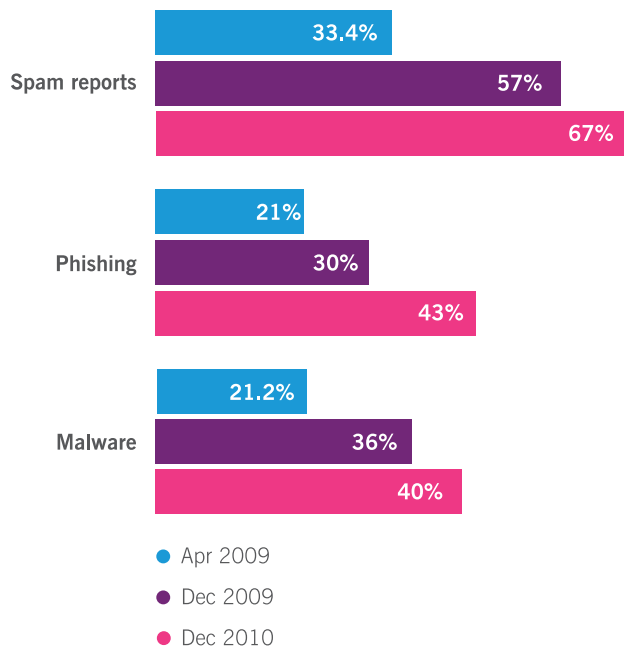


With furious debate raging every time privacy and security settings are tweaked on Facebook, it seems that functionality and ease-of-use triumph over security every time. For example, one of the latest innovations introduced is the automatic tagging of photos with the identities of those pictured. For individuals who like to [keep their personal details and activities private](#), this could easily be seen as an intrusion. And, even more disturbing is that automatic tagging could easily act as another gateway for malicious activity.

Spamming on social networks rose further in 2010, with 67% of people surveyed receiving spam messages, up from 57% at the end of 2009 and just 33% in mid-2009. Phishing and malware incidents were also rife, with 43% of users spotting phishing attempts and 40% receiving malware, plus it's likely that others are unknowing victims. This continues to cause headaches for businesses, with 59% of businesses worried that employee behavior on social sites could endanger company security.

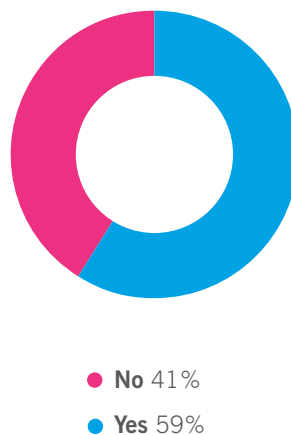
Fifty-seven percent of businesses think that employees maybe sharing too much information online. However, this isn't reflected in corporate policies. More than half of the companies surveyed imposed no limitations on accessing Facebook, Twitter and LinkedIn—and less than a quarter of firms completely block these sites.

Social networks Spam, Phishing and Malware reports up



Source: Sophos Survey December 2010

Do you think your employee's behavior on social networking sites could endanger security at your company?



Source: Sophos Survey December 2010

# Spam

As spam expands into other areas online, traditional email spam still remains a significant problem, especially in business. Workers still need to keep their inboxes clear of junk, and advanced mail filtering systems are a necessity in any business hoping to use email efficiently.

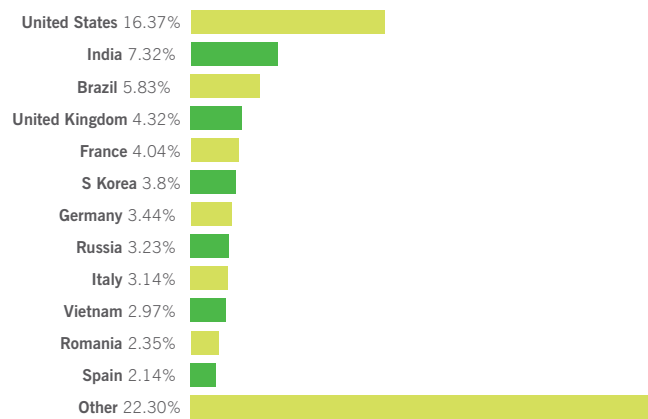
Spam generally relies on social engineering to lure its victims, using all the tricks including hijacking breaking news stories, and playing on human fears and desires. One of the biggest email scams is selling pharmaceuticals from offshore services. These emails promise to get around local drug control measures and [36 million Americans report purchasing drugs from online sellers](#). If these pharmacies really do exist and actually ship something to their customers—rather than simply taking the money and disappearing—purchasers put themselves at great risk, with the questionable safety of these drugs. Online shoppers also open themselves up to further scams, such as approaches from fake FDA agents threatening legal action.

With the convergence of spam and malware, a growing proportion of spam messages are moving away from these more direct scams. Sending out malicious attachments continues to be widely practiced, but even more prevalent is the mailing of links to poisoned webpages. Operating in the same manner as any other scam, victims are tricked into clicking a link in a mail and then led to a site that attacks their system with exploits or which attempts to [implant fake anti-virus software](#). 2010 also saw a surge in HTML attachments that directly point to malicious web content without directly visiting the dangerous sites.

*36 million  
Americans  
report  
purchasing  
drugs from  
unlicensed  
online sellers*

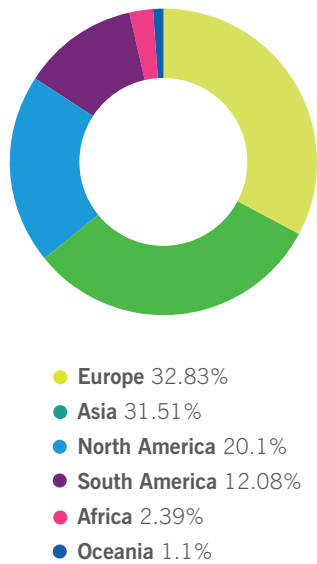
Spammers are also using more focused email scams, known as “spearphishing,” which sharpen the bait on their hooks to lure a specific target. Spearphishing notably targeted webmail services this year; businesses and institutions received warnings about problems with webmail services that turned out to lead to phishing pages. Once compromised, webmail accounts can become fertile ground for disclosing personal data, identity theft and corporate espionage.

Dirty dozen spam-relaying countries



Source: SophosLabs

Spam by continent



Source: SophosLabs

# Stuxnet

## Malware goes industrial-strength

One of the more widely-covered malware stories of the year concerned the “Stuxnet” worm. Stuxnet appeared to target highly sensitive SCADA systems, which monitor and control industrial, infrastructure or facility-based processes, and was remarkable for the sophistication of the code and the amount of work involved in its creation.

Some of Iran’s sensitive nuclear program computers were reportedly affected by it, which targeted programmable logic controllers, or PLCs. When Stuxnet found a targeted PLC, it injected its own code into it, concealed itself and the alterations it made; **Stuxnet caused the computer system to misdirect the controlled process.**

A report issued by the Congressional Research Service (CRS) claims that **Stuxnet could hit the U.S.** as well, hampering both the government’s capability and the society’s proficiency to protect the country. It states that a successful attack on the U.S. using latest variants of the Stuxnet weapon, can damage the country’s infrastructure including, water, electricity and transportation.

Enormous hype surrounded the discovery of the Stuxnet worm. The so-called military-grade malware may have been an advanced threat, showing a number of flaws in many layers of security processes, but we will **remember the Stuxnet worm** more for its media impact than its effect on global politics or industry.

# What puts **you** at risk?

Malware attacks can strike at anytime and from anywhere. Weak passwords, mobile devices and social networks, everyday software, removable media, operating systems and web all pose risk. We'll cover each of these access points in this section, so you know what puts your people and your devices at risk-and how to [thwart future exploits](#).



# Passwords

Despite the increasing sophistication and availability of alternatives, simple passwords remain the most common form of user authentication. Many online sites and services continue to rely on passwords alone to prove that the person interacting with them is who they claim to be. Weaknesses in this approach represent a serious hole in security.



Data-harvesting campaigns routinely steal passwords using malware or illegal technology like keyloggers and screenscrapers that monitor a computer user's activity. They're also occasionally leaked by poorly secured websites. The biggest such incident in 2010 affected [over a million users of several popular sites operated by the Gawker Media group](#), while [Mozilla's leak of 44,000 sets of logins](#) from its add-ons system seems to have only affected inactive accounts. Lost and stolen logins can be highly embarrassing—as experienced in 2010 by the usual roster of celebrities—but they can also be much more harmful when used to steal money or harvest sensitive business data.

The risk from phishing and spyware is by no means insignificant, but it is dwarfed by the danger people impose on themselves by failing to exercise proper password caution. Far too many people use simple and easily-guessed passwords like “123456,” “password” and “qwerty” as top picks from the Gawker leak. People also tend to use the same password for multiple sites, and change them rarely if ever.

To [prevent hackers from compromising your accounts](#), passwords need to be as long and complex as possible. They should use multiple character sets (letters, numbers and symbols) and avoid common words and phrases. You shouldn't repeat passwords from one site to another, and you should change your passwords regularly, especially for highly sensitive logins such as online banking. In business, hardware-based security methods, such as tokens providing one-time passwords, can help provide a much higher level of security. Banks and other providers of high-risk online services are slowly beginning to implement this type of technology.

*Far too many people use simple and easily-guessed passwords like “123456,” “password” and “qwerty”*

# Mobile devices and smartphones

According to Gartner analysts [one in six people will have access to a high-tech mobile device by the end of 2010](#). In the last few years, we've witnessed a radical change in the way we access and use the Internet. The rapid upswing in sophistication of mobile technology resulted in a swift change in the way we provide mobile content and interact with it. However, this change brings with it a wealth of new problems for security. In our new, always-connected age, maintaining the integrity and privacy of networks, business data and personal information is increasingly important and difficult.



# iPhone

Apple's iPhone kick-started the latest wave of touch-screen smartphones, setting the standard for both design and functionality. The only thing that matched the level of anticipation prior to the summer 2010 release of the fourth generation of iPhones was the [extent of spammers' exploitation](#) of the news. A wave of spam messages offering free phones, just hours before Steve Jobs' official public unveiling, [shadowed the actual release of the new iPhone](#).

We've seen gradual improvements on the level of security on iPhones since its first release. Many companies that once considered iPhones unsuitable for business use are now changing their minds. Nevertheless, active threats continue to loom. Despite no major outbreaks seen last year, early in 2010 hackers released the source code for [potential iPhone spyware](#) to the Internet (this also affected BlackBerrys). They followed this with the demonstration of a [proof-of-concept botnet made up of iPhones and Android devices](#); the trick persuaded close to 8,000 users to join before researchers unveiled it.

Early 2010 also discovered potential issues with encryption. Apple stepped up efforts to keep up with newly emerging vulnerabilities in their operating system and software. They released an upgrade to the core iOS [covering some 65 vulnerabilities noted in previous versions](#), with a [further batch of fixes issued just](#) a few months later.

The majority of security issues continue to focus on jailbroken devices, where the mobile security settings are unlocked to get more functionality. The [JailbreakMe.com website made iPhone jailbreaking easier](#) as it exploited security vulnerability in the way the iPhone's version of the Safari browser processed PDF documents to unlock the phones with minimal user effort. Apple released a patch a week or so later, but users continue to jailbreak their devices in droves, tempted by the possibility of installing applications not approved by the company. However, by doing this, users circumvent the iPhone's principal security measure.

By the end of the year, a computer consultant developed an optional added layer of security for jailbroken phones, providing [Address Space Layout Randomization](#). However, no method of securing phones will provide a complete protective arsenal, as hackers continue to develop ways to subvert devices. The sheer dominance of Apple's devices in the smartphone market, and the diverse range of uses they can be put to, also make iPhones prime target for mobile cybercriminals.

Jailbreaking is a bad idea, as it undermines Apple's inherent security model and opens the user to more risk from social engineering tricks. Even with fully secured phones, users need to exercise normal precautions against scams, and keep an eye out for the usual tricks and lures.

iPhone risks can be mitigated if you exercise caution. When iPhones are plugged in to home or company computers or are set up on unapproved wireless networks to provide phone connectivity, threats are transferred from the iPhone to more vulnerable systems and networks. You can use a blend of policies and technologies to keep your network and machines safe. ["Acceptable use" policies](#) can attempt to control what users plug into home or company devices together with quality anti-malware at the desktop level and [solid device control](#) network-wide.



# Android

Google's Android tried to keep pace with the iPhone in terms of functionality, and as devices diversify, the Android user base continues to grow. In early in 2010, Google found and removed banking malware from the site when a wallpaper application [gathered information on over 1 million Android users](#). Researchers at the BBC put together their [own smartphone spyware](#) with ease and researchers spotted a basic SMS Trojan in Russia, although it didn't make its way onto the Android market.

The more open nature of the Android app market and the design ethos of the operating system make the Android more exposed to attack than the locked-down iPhone. The Android's ability to run Flash means updates to Adobe applications are required.

Some components are built-in parts of the operating system, and therefore require full OS upgrades to patch vulnerabilities; this causes issues for some older devices [that can't run newer editions of the platform](#). The openness of the Linux-based platform makes it possible to access and tinker with low-level components, but also attracts more research into possible flaws and how they might be exploited for profit.

All in all, Android phones represent a considerable exposure point, but again one that relies heavily on social engineering to lure users into installing rogue or malicious applications that give the bad guys access to their phones. Keeping alert and well-informed on the latest scams remains one of the most important aspects of staying secure.



# Windows 7 phone

We saw the release of Microsoft's latest mobile platform, Windows 7 phone, in many regions in late 2010. The platform's clear advantages for interaction with existing business software such as Exchange, make it likely that the Windows 7 phone will be a particularly strong player in the business market, which is currently dominated by RIM's BlackBerry. The need for flexibility and cross-hardware support makes it difficult to implement Apple-style lockdown and Microsoft's reputation for favoring functionality over security does not bode well for security on the devices.

# BlackBerry

RIM's BlackBerry is still the device of choice in corporate environments, if much less popular for personal purposes. The BlackBerry security-built-in model is fairly successful so far, although [potential spyware applications have been introduced](#). Most new developments—if anything—weaken that security model, with several nations pressuring RIM to slacken their policy of transporting all data through their central servers in strongly encrypted form, preventing government snooping on traffic. Only time will tell if the security model will be diluted or compromised by the discovery of vulnerabilities, and users should avoid placing too much trust in these devices simply because today's security model is effective.



# Other mobile platforms

With Apple, Google, Microsoft and RIM dominating the headlines in the next-generation smartphone market, other major players are working hard to catch up. The Palm Pre is keeping up with demands for broader functionality, and finding the same [problems maintaining security](#). A flaw exposed this year granted cybercrooks a backdoor into Pre systems via a maliciously-crafted mail message or webpage.

Meanwhile, despite losing market share to more advanced models, mobile giant Nokia's relatively humble Symbian operating system continues to hold a massive share of the smartphone market. We continue to see a notable quantity of real working malware on the Symbian operating system due to the combination of a large pool of potential victims and a relatively insecure operating model.

Fortunately, there are quality security solutions that can protect against these threats, and it seems likely that as newer and more sophisticated devices become more widespread, these older and less secure platforms will slowly die out.

# Social networks



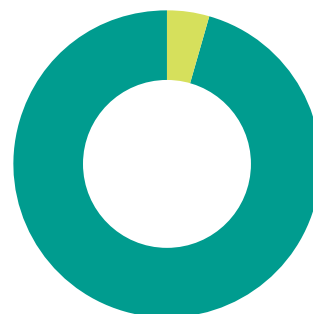
# Applications

Facebook, by far the largest social networking system and the most targeted by cybercriminals, has a major problem in the form of its app system. Any user can create an application, with a wide range of powers to interact with data stored on user pages and cross-site messaging systems, and these applications, like survey scams, can then be installed and run on any users' page.

To combat this serious problem, a "walled garden" approach may be more suitable. This refers to a closed or exclusive set of information services provided for users, in contrast to allowing open access to applications and content. This is the way the Apple App Store operates, with applications requiring official approval before they can be uploaded to the site and shared with other users. It has proven effective in protecting users from maliciously crafted applications. Facebook users responding to a (legitimate) survey also approve of this approach.

Another option would be to give those users with security concerns the option to secure their own page, allowing only vetted applications to run. This second approach would only protect the more aware and cautious of users, who may be less likely to fall for the scammers' social engineering tricks anyway. It wouldn't do much to reduce the spam flooding from less secure users, and a full-spectrum control system is preferable. Of course, even official vetted and approved applications can't be entirely trusted, with the occasional slip allowing applications that harvest user data to make it onto the verified lists.

Should Facebook follow Apple's example and have a "walled garden" verifying all apps?



- **Yes** it would be better for security 95.51%
- **No** there shouldn't be restrictions on what apps are written 4.49%

Source: Sophos Poll October 2010

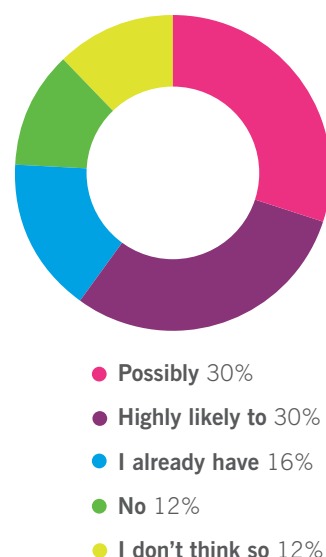


# Privacy settings

In addition to the application problem, Facebook comes under regular criticism for its provision, implementation and explanation of user privacy features. Directions for setting privacy preferences are vague and unclear—if and when they're provided. Plus, once uploaded, information and content may be difficult or impossible to remove.

Facebook and other social network operators would be well advised to impose a comprehensive “opt-in” system for all user content. This would make it clear exactly what will be visible to whom and force users to make an explicit choice of how open to make their information. Such an approach would drastically improve the security of potentially sensitive information. And, doing it proactively, rather than waiting for legislation to force the issue, would engender increased trust in the safety of the system and respect for its operators.

Do you think you will quit Facebook over privacy concerns?



Source: Sophos Poll May 2010

# Insecure infrastructures

A [cross-site scripting \(XSS\) vulnerability in the Twitter](#) website also put users at risk in 2010. This vulnerability allowed links to be posted with embedded JavaScript code known as “onMouseOver.” It displayed pop-ups and third-party sites when a user merely hovered over a link without even clicking on it. Hackers exploited this vulnerability, in many cases simply for pranks, but also with more malicious intent.

The issue only affected certain browsers, and Twitter moved quickly to protect their users. The weakness did not affect most users accessing the system through third-party, but the incident highlights the need for close attention to possible vulnerabilities when building a web service for a mass user base.

# Software

We all require software to help us in our daily work and personal communications. Software is just as likely to contain insecure code and vulnerabilities that allow malware spread.



Cybercriminals tend to target Microsoft, because its Office and Internet Explorer solutions are ubiquitous. Many users view this software as an integral part of the Windows platform, rather than separate software that may need a separate regime of updating and patching. Lately, cybercrooks targeted Adobe to enable malware distribution, as its PDF Reader and Flash player are also widely, if not universally, installed.

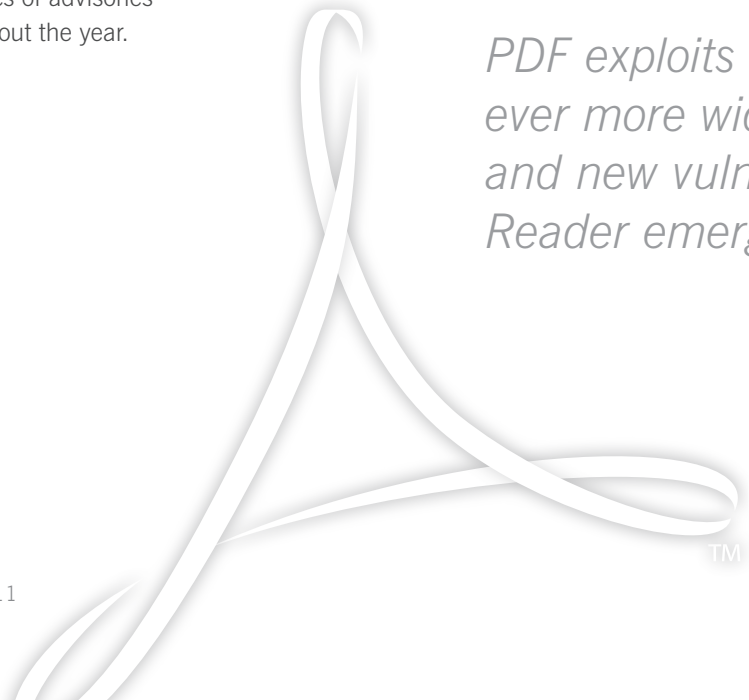
Researchers have noted problems with Adobe PDF documents for some years now, since the ability to run active scripts is enabled by default in Adobe's Reader software. In 2010, PDF exploits became ever more widespread, and new vulnerabilities in Reader emerged regularly. Maliciously-crafted PDFs are placed on websites or mailed out in spam runs, hoping that they will be opened in vulnerable Reader software and their payloads will be given free rein to infect systems.

With more and more websites using Flash to display dynamic imagery and more users installing the required player software (itself a common trick to get Trojans installed), Flash problems are also becoming more widespread. New zero-day exploits and critical patches for Adobe software became routine in 2010 with a series of advisories and patches issued throughout the year.

Amid all this activity, and increasing calls for action such as disabling JavaScript by default, [Adobe showed signs of moving towards better security](#). In 2010 they added [automatic updating capabilities](#), and will add, "sandboxing" in new versions of their Reader solutions. The companies hope that this effort will isolate malicious scripts from the local system. We'll know their success with time.

Other popular Adobe packages such as Shockwave and Photoshop also needed to address security concerns in 2010 and required patching. Java, produced by Sun Microsystems, and now part of Oracle, also drew a lot of attention from malware writers due to its wide installed base, with an [increase in exploits included in malware observed](#).

In many cases, malware exploiting these vulnerabilities led to fake anti-virus software scams, but cybercriminals also used PDF attacks to link to more complex chains of malware infestations such as the [Salinity virus family](#).



*PDF exploits became  
ever more widespread,  
and new vulnerabilities in  
Reader emerged regularly*

TM

# Removable media

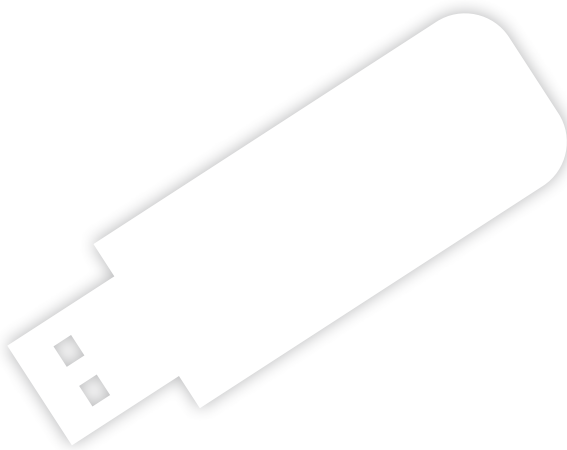
Though we'd like to think removable media, such as flash drives, network cables and Wi-Fi connections have replaced discs, they're still used and remain a significant exposure point.



# USB flash drives

The USB flash drive is now the method of choice for easy sharing of files between people in the same physical location. Fast, capacious, robust and cheap, they're in widespread use in just about every sphere of computing. And of course, they've become a prime target for malware authors. Modern malware—including high profile examples such as [Conficker](#) and Stuxnet—exploit USB drives to automatically run when inserted into a target computer. Stuxnet took it one step further and exploited an unpatched security vulnerability to bypass even the need for “AutoPlay” to be enabled.

Targeted attacks also frequently use this threat, notably the social engineering trick of dropping infected sticks in company parking lots, hoping that curious employees will pick them up and insert them into company systems, breaching the corporate network boundary. Flash drives are also commonly given away as freebies at trade shows, a practice which makes for major embarrassment if inadequate security procedures are carried out. IBM learned this this year when the complimentary USB drives it handed out at the AusCERT security conference in Queensland, Australia were [infected by not one, but two pieces of malware](#).



## CDs/DVDs

While permanent media such as CDs and DVDs don't provide as much opportunity for infection by malware authors, they can still transmit malware—whether explicitly infected or accidentally when copying files onto the disks.

The media is most risky as a data loss format. It's easy for disgruntled employees to download valuable data to CDs and DVDs and walk out the door, as the U.S. government learned this year when data sneaked out in this way sparked the ongoing WikiLeaks saga.

## Other plug-and-play devices

When considering USB drives and CD or DVDs as means of moving data around, it's easy to discount the range of other devices with similar properties. Camera memory sticks, GPS devices and even smartphones all contain flash-based storage, which is fundamentally the same as a standard thumb drive. These plug-and-play devices are just as capable of containing malware and the associated AutoPlay and other exploits, and are thus likely to fall victim to malware as well.

Plug-and-play devices are a subtle way of sneaking contraband data past normal security checks, and are less likely to be analyzed than more recognizable forms of moving data around. Therefore, they need to be subject to the same access control and data loss prevention procedures as flash drives.

When factories have poor quality control procedures, [removable devices can come “pre-infected” with malware](#). A machine used to build, install or test hardware can become infected and passes on the infection to each device it comes in contact with; this can be highly embarrassing to product vendors and result in costly recalls.

# Operating systems





# Windows 7

Overall, Windows 7 provides a secure environment, but there's still room for improvement. When the first few versions of Windows XP came out, there were much more serious issues than with Windows 7—and many were fixed with Service Pack 2. [Microsoft plans to release Windows 7 service pack 1 in 2011](#). However, numerous security fixes have been already released as part of the Patch Tuesday program.

Usage statistics show a steady uptake of the new OS; it is rapidly catching up with Vista and looking certain to overtake it as more new machines come pre-installed with Windows 7 and as older operating systems, including the no-longer-supported XP SP2, fade away. Malware creators are now starting to hone their attacks to [specifically-target Windows 7](#), particularly the ubiquitous [rogue security solution scams](#), and this trend will continue as the platform and its users become an ever larger target.

*Malware creators are now starting to hone their attacks to specifically-target Windows 7*

# Mac

Many people consider Apple's Mac OS X platform to be more secure than Windows. Some believe that its UNIX-based approach to privileges and permissions grant it a firmer security footing than Windows, and the more limited range of hardware support required means less code and therefore less exposure to code vulnerabilities.

Since fewer Macs are used in corporate environments, the Mac is a smaller target upon which cybercriminals can focus. As a result, the Mac malware problem is a tiny fraction of that seen on the Windows platform. Nevertheless, malware continues to emerge on a regular basis. And even without as many opportunities to infect and spread across platforms, Mac users are still vulnerable to the scams and tricks used to persuade and pressure them into installing suspect software, to open up their systems to remote access, or to hand over their sensitive data.

For example, 2010 saw a new version of the [OSX/Pinhead Trojan](#), which poses as a copy of the iPhoto application distributed with all new Macs. If the user is tricked into installing the software, it opens up a backdoor allowing crooks full access to the compromised system. Later in the year, the [Boonana Trojan targeted Mac](#), Windows and even Linux users. It spread through spammed links on Facebook and used standard social engineering tricks to lure victims into installing a Java application, which downloads and runs a further torrent of malicious applications.

Apple is working harder to protect users against "Trojanized" software through the upcoming with Mac App Store, due to go live in early 2011. Operating along similar lines to the iOS App Store which provides applications for iPods, iPads and iPhones, it's set to become a central repository and sales system for all Mac software, introducing a level of security checks to ensure that software behaves as desired. The impact of this will depend on how widely Mac users adopt it, but it's unlikely to provide the same level of safety and control that the iPhone enjoys. Users will almost certainly still be able to access and install software from anywhere else they may find it, and this leaves them open to the full range of social engineering tricks and vulnerabilities.

With malware writers taking advantage of any potential security hole, it's just as important for Mac users to keep up to date with patches as anyone else. The fact that these patches exist at all may be seen as proof that the platform is far from air-tight. In a single release in November 2010, Apple patched 100 different vulnerabilities.

With many Mac users paying little heed to security—due to their sense of invulnerability—the Mac community was well served in 2010 by the release of a [free-for-personal-use anti-virus solution](#), along the lines of several similar offerings available to Windows users. Within days of its release, the new solution spotted a range of infections, and has also shown that while many Macs may not often be actively infected with malware, they can still be carriers for [Windows malware just waiting to cross-propagate](#).

Computer users often overlook the risk of transferring infections from one platform to another, but this problem can present a significant penetration point both at home and in business. All systems need to be kept secure and running quality security software, regardless of whether or not they themselves are considered susceptible to infection. In businesses with multiple platforms working together it's especially vital to have strong policies regarding securing of all platforms and enforcement systems to [ensure compliance](#).

*Mac malware problem is a tiny fraction of that seen on Windows. Nevertheless, malware continues to emerge on a regular basis*



# Web server security threats

Despite the continuing presence of threats via movable hardware, the web is by far the biggest opportunity for malware infection. It transmits emails bearing malicious links and attachments, websites carrying exploits targeting browsers and other software, drive-by downloads, phishing scams, questionable storefront operations, and all the other malice of the cyber world.



# Malvertising

One of the growing issues of the past year is “malvertising”—the implantation of malicious advertisements onto websites. In many cases, the websites are entirely innocent and unaware of the threat they’re posing to their visitors. Malware advertising is slipped into feeds from external advertisement resellers and appears alongside the standard set of ads. The infiltration may exploit flaws in ad-server software, or may be accomplished by concealing the malicious activities of ads in order to get them past checks run by ad suppliers.

In 2010, malvertising appeared on the websites of [Minnesota’s largest newspaper the Star Tribune](#), the popular [online game Farm Town](#) and even in the sponsored links accompanying Google search results. In all of these cases, the [malvertising led to fake anti-virus software scams](#) aiming to trick victims into paying to clean up non-existent malware infestations. Scammers often presented these malicious advertisements through links designed to look like legitimate ad sources.

*the websites themselves are entirely innocent and unaware of the threat they’re posing their visitors.*

# Compromised legitimate websites

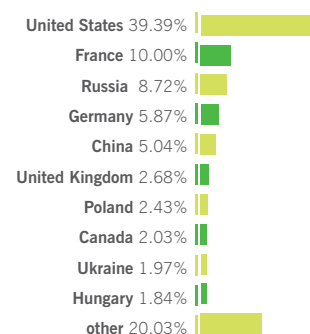
Compromised legitimate websites can introduce malware and scams. We see 30,000 new malicious URLs every day. That's approximately one every two to three seconds. And, we've found that more than [70% of these are legitimate websites that have been hacked](#) or compromised. Criminals gain access to the data on a legitimate site and subvert it to their own ends. They achieve this by exploiting vulnerabilities in the software that power the sites or by stealing access credentials from malware-infected machines.

The uses for compromised sites are diverse. In 2010, cybercriminals used compromised sites for standard drive-by downloads of malware, including “ransomware,” which encrypts important files and demands payment for the access codes. Another example is to demonstrate weaknesses in [supposedly secure sites holding personally identifiable information](#). Compromised sites include the European site of [popular tech blog TechCrunch](#), news outlets like the [Jerusalem Post](#) and [local government websites](#) like that of the U.K.'s Somerset County Council. The crooks even hit major hosting providers, and once compromised they can cause all sites they [host to serve up malware](#).

Twitter feeds also became an increasingly popular target for malicious takeover in 2010. As Twitter becomes an ever more prevalent means of spreading information—personal, commercial and official—popular feeds are a simple way of getting access to large crowds of people. Leading feeds are used to [tweet links to scam websites](#). In one particularly malevolent case, hackers used Twitter to spread hoax emergency warning messages from an [official disaster advisory account in Indonesia](#).

Celebrity Twitter feeds are a particularly juicy target thanks to their predictably large followings. In 2010, prominent TV presenters, politicians, rock stars and rappers all had their [Twitter accounts hacked](#) by spammers. In a similar vein, hijacked email accounts make fertile ground for spreading spam and scams. Email that seems to be coming from a trusted source is more likely to be opened; and as a result links are clicked on or attachments opened. [Breaches in account security can have serious consequences](#). U.S. Vice Presidential candidate Sarah Palin commented in a book published in late 2009 that a [hacker breaking into her personal Yahoo! account](#) “created paralysis” in her campaign camp because it cut off easy communication with her colleagues in Alaska.

Top ten countries hosting malware



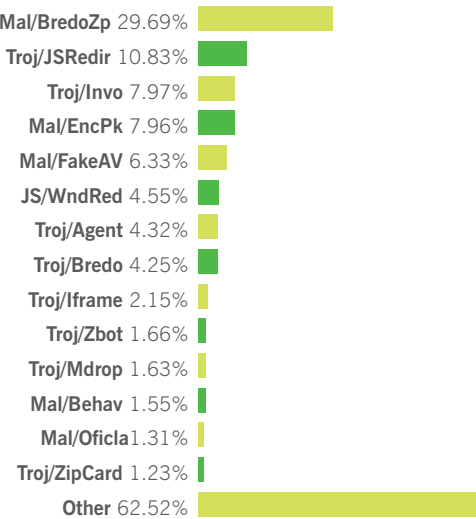
Source: SophosLabs



# Email spam

Email spam remains a significant path for threats, simply because the vast majority of computer users still use this medium. Spammed emails containing attachments remain a popular tactic for cybercriminals, often taking advantage of vulnerabilities in Office and PDF Reader software to launch malicious code from within innocent-looking document formats. Emails containing links to malicious sites continue to increase as a major means of leading new victims to attack sites, operating in parallel with SEO-based lures.

Top malware spreading via email attachment



Source: SophosLabs

# Zero-Day threats: what are they, and how to avoid them?

In a nutshell, “zero-day” threats are attacks that make use of vulnerabilities, which are not yet patched. This usually means that malware writers or vulnerability researchers find a flaw in some piece of software, which can be used to bypass some security measure and get malicious code to run. For example, bugs in browsers can mean that rather than simply displaying a webpage as they should, carefully crafted webpages can cause malicious code to be executed on your computer. Similarly, bugs in PDF Reader software can mean that code can launch from inside PDFs.

While the name zero-day implies a single day, the window of opportunity for a zero-day threat runs from the moment the vulnerability is first discovered to the time the software developers provide a patch or update to cover the hole. From a user’s point of view, it runs until the patch is fully applied; until then, the vulnerability remains open and the threat can compromise the users’ system. When vendors are slow to patch flaws, third parties may develop patches or workarounds to mitigate the threat.

In many cases, vulnerabilities are discovered by honest security researchers and pointed out to the software vendors to fix. In some cases, if a fix isn’t timely, the issue may be made public to encourage more prompt patching. In other cases, criminals may come across problems, and exploits may be sold between gangs of cybercrooks on the black market. Working exploits for genuine and unpublished zero-days are particularly valuable to attackers.

Tools are available to protect against zero-day exploits. One such tool is a buffer overflow prevention system, which should be included with quality multi-layer security solutions. To keep the zero-day window as small as possible, you should patch promptly and apply all recommended workarounds. In many cases, flaws will only affect software with certain settings enabled or disabled, and a secure approach to configuring all software should be a core part of any corporate security strategy.

# Tablet evolution

Apple's much-vaunted iPad introduces a new attractive way to use a computing device. Although early models are little more than an enlarged iPod touch, the spectacular popularity of the iPad indicates that the time has finally come for the tablet format to compete with the Netbook and the smartphone for mobile computing market share. Similar to the iPhone, cybercriminals hijacked the huge interest in the new devices, with offers of free iPads flooding email inboxes and social networks. Of course, almost all of them lead to phishing, malware, or scams.

Interestingly, Apple has resolutely refused to allow its mobile devices to run Flash applications. Perhaps, this is in part due to the upturn in security problems in Adobe software, but officially the reason is merely to avoid inefficient and power-draining technologies. News emerged in the summer of 2010 that "frashing," a technique for persuading unlocked iPhones to run Flash, is possible for use on iPads too. As this is likely to encourage more owners of the devices to unlock and hack their machines to enable access to a wider range of content, it enables more threats targeting those who chose to bypass some of the lockdown security features built into the devices.

Many hardware manufacturers responded to the iPad launch with competing products; among the first to market were tablets running the Linux-based Android operating system, such as Samsung's Galaxy Tab. Windows versions are also due soon, including the EEE Pad from Asus, with expected availability in early 2011.

Full-scale computing power together with always-on, anywhere-anyplace-anytime connectivity and a more casual attitude towards computing, brings with it potential dangers. The potential for deception and the sloppiness of a finger-powered control system (versus a standard keyboard and mouse) are additional concerns. We expect more cybercriminals to target iPad users in the upcoming year.

# Protecting yourself from current and future threats

Today's legal system is dealing with cybercrime, but just barely. Your best defense should include a combination of common sense decisions and protection software. Businesses and end users should employ this type of multi-layered approach to avoid becoming the victims of malware.



# Legislation and criminal justice

If you measured the Earth's history in geological timeframes, the entire history of human civilization registers barely more than the blink of an eye. Similarly, in legal terms, issues of malware, spam and cybercrime are still considered very new and haven't been fully addressed by adequate global legislation. Nevertheless, 2010 saw some advances in the arrest and prosecution of cybercriminals, with promising signs of cooperation and data-sharing between national and regional police forces. This is a vital step in combating crooks to which national borders represent little more than something to hide behind.

In something of a bumper year for the tracking down and punishment of the cybercriminals, March saw the creator of the [Allapple worm](#) sentenced to 2 years and 7 months in Estonia, while in July the gang behind the ["Mariposa" botnet came under investigation](#) and the FBI and police forces in Spain and Slovenia arrested the 23-year-old ringleader in a joint operation. In August, officials arrested a Japanese malware writer under suspicion of creating malware, which spread through the Winny peer-to-peer system.

In the second half of 2010, police broke up another gang of botnet operators, with 19 arrests in the U.K., 60 charged in the U.S. and further police action in the Ukraine. This was all in connection with the [notorious Zbot \(or Zeus\) botnet](#), thought to be responsible for the theft of over \$200 million. In late October, Dutch police announced the successful takedown of the [Bredolab botnet](#) and police in Armenia picked up a man thought to be behind the operation.

On a smaller scale, the courts sentenced a Scottish man to 18 months imprisonment for distribution of [data-stealing malware](#), both for financial gain and, according to the trial judge, to get pleasure from intruding into the privacy of others. Law officers discovered that a contract worker at the U.S. financial institution Fannie Mae planted malicious scripts in the firm's systems, designed to destroy data at a fixed date in the future in order to cause huge damage. The courts sentenced the hacker who hijacked Sarah Palin's email account to over a year in jail, and the U.S. Secret Service picked up a man who broke into the systems of the Federal Reserve Bank of Cleveland—as well as stealing over 400,000 sets of credit and debit card details from several other banks. In the world of social networking, Facebook announced lawsuits against the operators of the [survey scams](#) plaguing its site.

More arrests were made in the online gaming world, with two suspects picked up in Japan in relation to theft of login credentials for popular game, Lineage II, [using spyware planted on victims' systems](#).

The gaming world was also hit by one of the most widely-reported attack techniques of the year, with a 17-year-old arrest in the U.K. under suspicion of involvement in Distributed Denial of Service (DDoS) attacks on servers running the 'Call of Duty' shoot-em-up game. Another attacker was sentenced for using university systems to launch [DDoS attacks on the websites of right-wing politicians](#).

The major DDoS stories of the year however were related to the WikiLeaks scandal. After the release of large amounts of politically-sensitive data by the whistleblowing website, and the subsequent decision by several payment systems to cease procession donations to the site's operators, a hacker group took it upon themselves to retaliate, without the support of those running the site. The 'Anonymous' group launched attacks on the servers of several payment processors involved, and encouraged others to join in using publicly-available attack software.

With [DDoS attacks illegal in many regions](#), those participating in the retaliatory action were open to litigation, and in the Netherlands police arrested a 16-year-old boy in relation to the campaign. Attacks then turned their attention to the Dutch police websites, leading in turn to a second arrest. Another DDoS attack rumored to be related to the story, [against perennial DDoS targets Spamhaus](#), was found to be unconnected. Amidst all the political posturing, many observers lost sight of a significant chapter in the whole saga, the original data loss, apparently accomplished by copying vast swathes of data to a CD and walking it out of a building. Given the supposedly sensitive nature of the data involved, this should have been made far less straightforward a task, with proper data security systems and procedures.

*'Anonymous' group launched attacks on the servers of several payment processors*

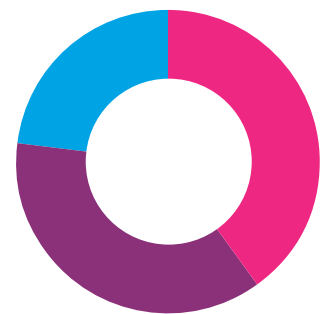
# Measures taken by government to combat cyberwarfare

Hollywood screenwriters continue to show us the prospect of cyberwar and cyberterrorism on film. But, are these threats based in reality? Some, including security guru Bruce Schneier, see this as a [distant and over-hyped threat](#). Yet, 2010 could be the year that saw the first real glimmers of a spark in the bonfire of global cybercombat, with three major incidents.

What later became known as “[Operation Aurora](#)” marked the first days of 2010. This major offensive targeted Google, Adobe and many other large companies with the apparent goal of accessing webmail accounts of Chinese human rights activists. And many believed the source to be China. The Chinese government denied involvement, and many dismissed the incident as large-scale corporate espionage, but it sparked a major human rights disagreement and brought responses from many national governments. The U.S. Secretary of State issued a statement after a briefing by Google on the incident, and shortly afterwards the German and French governments issued advice to [avoid using Microsoft's Internet Explorer browser](#) because it was vulnerable.

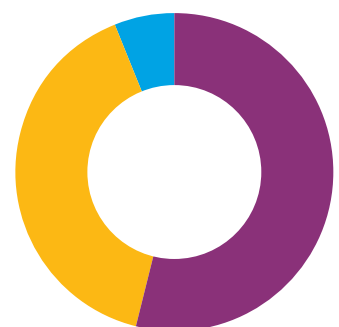
Later in the year, the emergence of the [Stuxnet worm](#) hinted at the potential of [malware to attack](#) and subvert exactly the kind of sensitive national infrastructure the conspiracy theorists have long suggested as a prime target. Then, as 2010 drew to a close, the WikiLeaks saga combined data loss, political scandal and international, orchestrated attacks conducted through the Internet. These attacks focused on financial institutions and websites promoting regional governments and institutions, but along with the other components in this trio of events, they highlight possibilities, which have been hovering over the web for some time.

Do you think it's acceptable for your country to spy on other countries via the Internet by hacking and/or installing malware?



- Yes, but only in wartime 40%
- No 37%
- yes 23%

Is your country doing enough to protect itself from Internet attack by another nation?



- No 54%
- I don't know 40%
- Yes 6%

Source: Sophos Poll August 2010

# Measures taken by businesses

Cybercrime is encroaching more and more into the business space. Industrial espionage, spearphishing of important employees to breach network boundaries and mass theft of customer information are more difficult to detect and have very serious consequences. At the same time, network boundaries are becoming ever more indistinct and porous as new technologies enable greater access from remote workers and mobile devices. In addition, legal requirements place greater emphasis on traceability and compliance with predefined standards of data hygiene.

Increasing amounts of sensitive data is stored, accessed and manipulated in databases connected to company websites as businesses increasingly interact with their customers through the Internet. As a result, it's become as easy to access these databases as it is to access the main doors at corporate headquarters.

Security administrators face a constant battle to maintain usability, while preventing penetration from the outside and data loss from within. Alongside protecting network boundaries, businesses and website maintainers are under growing pressure to ensure that their web presence provides adequate protection for the users of its web services.

*legal  
requirements  
place greater  
emphasis on  
traceability and  
compliance*

Social networking sites are particularly exposed in this area. Users trust these sites with vast amounts of often highly sensitive information. The amount of data that can be harvested by cybercriminals is dependent on both the way sites are designed and run, as well as the security underlying the site's software. There's no need for hackers to break into web servers and harvest user data if the users upload useful information for all to see. Many social media sites focus more closely on growing their numbers of users, rather than ensuring users are kept safe and fully understand their privacy systems. As a result, many social networking sites are rife with malware, spam and data harvesting. Operators of social networking sites and web resources need to keep their customers safe in addition to keeping them happy.

Meanwhile, security providers must continue to innovate and improve their services and solutions to ensure best possible protection is available. With the never-ending increase in volumes of malicious code and threat-serving webpages, it's becoming increasingly impractical to treat solutions as standalone, independent software. In addition, many leading developers are extending their solutions to the cloud. Although this has its benefits, it also opens up a full spectrum of dangers, which require additional protection. Investment in expert systems to rapidly and accurately spot, analyze and [classify newly emerging threats](#) is a must.

# End user education

A lot of the scams and social engineering techniques discussed in this report aren't new, and are certainly not unique to the cyberworld. Since the dawn of civilization, con artists, mentalists and tricksters have deceived and exploited innocent victims for profit. It seems inevitable that some people will fall for convincing stories and plausible tones no matter how strongly they're warned to be on guard.

However, the speed and reach of scams has been magnified enormously with the rise of the Internet, mass email and social networks. Now, a single scammer can try their luck with millions of targets at once. An email campaign can carry a link to vast numbers of inboxes, and only a few people need to be lured into following the links for the scammer to profit. By just clicking on a link, a user's machine can become infected, their personal details can be harvested or they can be led to a dishonest online retailer seeking to turn a profit from the effort.

Of course, the speed and reach of the Internet works both ways. It enables warnings and protective measures to be disseminated worldwide at lightning speed too. Educators and threat watchers are warning a growing audience of alert listeners. And, as more people become aware of the dangers of the web and [learn to keep an eye on the latest scams and threats](#), we all steadily become safer.

There's still a long way to go. Too many people are too willing share anything they can think of on their social networking pages, with no thought of the possible consequences. And many people unthinkingly click on an email attachment or link because it comes in from a friend or colleague's email address.

We need to balance caution and sensible precautions with usability. Users need to be able to trust that online purchases and other payments will be safe and secure, that their banks will look after their money and that their purchases will reach them. Without this trust, we would be afraid to communicate or conduct any transaction online. Yet, as Ben Franklin's old adage says, "An ounce of prevention is worth a pound of cure."

Businesses and service providers have an opportunity learn from the scams and exploits of the past in order to strengthen their defenses and offer the best security and reliability possible.

*"an ounce of prevention is worth a pound of cure."*

*Ben Franklin*

# What tools help us to stay secure?

While **education and awareness is the best way to stay ahead of the bad guys** and malware attacks, there are also a range of technologies you can employ to help maintain security and privacy. They include:

**Anti-virus software:** a must-have for just about any computer system. Detects, blocks and removes malicious code; should cover **rootkits**, scripts in webpages, exploit attempts and other malicious activities as well as traditional file-based threats. Local detection data best supplemented by expanded online lookup systems to efficiently protect against the latest emerging threats, and use whitelisting to minimize serious false positives.

**Gateway malware and content filters:** watch for malware being downloaded, at the gateway level. Should be blocking malicious URLs as well as file transfers, again using cloud lookups. **Quality web filtering solutions** will enable enforcement of corporate browsing policies too. Management and reporting systems will help corporate admins monitor company networks and ensure compliance with policies.

**Anti-spam software:** another must, especially in business. Filters email to remove spam, phishing scams, messages with malicious attachments and links to malicious webpages. Must combine strong detection with vanishingly small false alarm rates. Should also provide traceability and archiving to ensure blocked messages can be retrieved in case of problems.

**Encryption software:** Vital in any business working with sensitive customer data, and in many places where internal data might be valuable or compromising if lost. Data should be kept in encrypted form whenever possible, particularly during transfer and on portable systems or devices. Failsafes and administrator overrides are also useful in case of lost passwords or abuse by rogue employees.

**Patching and vulnerability monitoring:** All software needs to be kept up-to-date with the latest security fixes some may offer automatic updating, but in corporate environments internal testing may be needed first. Solutions are available to coordinate and enforce patching policies across a network, and tools can also scan **for vulnerable and out-of-date software.**

**Device and network control:** Enforcing rules on which systems and devices can connect to company networks is a necessity to ensure network integrity; company networks need to be isolated from all potential sources of infection, and should also be protected from methods of data theft.

**Data loss prevention:** Sensitive information can be specifically walled in and prevented from moving off of designated systems where it's needed; this stops malware or rogue employees from stealing company or customer information.

# How to stay ahead of threats

2010 saw the continuation of a long-term shift in the way we use our computers, and the way they're integrated into how we conduct both business and our personal lives. As a result, the bad guys are focusing more and more on social engineering tricks and social sites to find and exploit new victims. As the devices we carry and use—and the functions they offer—evolve and expand into every sphere of our lives, all the dangers posed by connecting to global networks also continue to grow in both scale and sophistication.

With the increasing organization and capitalization of cybercrime, the various methods and techniques used to implant malware, spread junk marketing and target scams have merged. In many cases, there's no boundary between spam, scam and malicious software; they all operate together in a simultaneous assault on the victim, their computer and their information. New techniques and methods may emerge, and old ones come in and out of fashion, but underlying it all is a similar set of principles. Software and operating systems have vulnerabilities, and to exploit them it's generally necessary to trick users into doing something they shouldn't. This is usually managed by taking advantage of human psychology.

Technological defenses against cyber threats have also evolved and improved of course. Well-implemented, quality solutions can provide a very solid protective barrier, including blocking or at least warning users against attempts to trick them. It's vital that users are well-educated on what might threaten them, and how best to spot and avoid the scams and tricks.

However, it's just as important that technological protective measures are designed with as close an eye on human psychology as the threats they're battling. Security measures that are difficult to implement, operate or use are likely to impact productivity. They are also likely to be subverted, bypassed or simply disabled by users and administrators who find them obstructive, awkward or plain irritating.

At the root of cybersecurity, it's all about people. Computers are simply devices to enable and simplify things people want to do, and computer threats are no more than attempts to trick people, or their computers, into doing things the bad guys want them to. Understanding of the threats, the threat methods and the tools we can use to protect ourselves now and in the future is the best and simplest way to minimize the danger.

*the bad guys are focusing more and more on social engineering tricks and social sites to find and exploit new victims*

*Understanding of the threats,  
the threat methods and the  
tools we can use to protect  
ourselves now and in the  
future is the best and simplest  
way to minimize the danger.*



**Sources:**

[Naked Security](#)

[Sophos.com](#)

[SophosLabs](#)

[Gartner Information Technology Resources](#)

[The Register](#)

[The Georgian Daily](#)

[BBC UK](#)

[The New York Times](#)

[Whatis.com](#)

[Microsoft TechNet](#)

[Cnn.com](#)

Copyright 2011 Sophos Ltd. All rights reserved.

Sophos and Sophos Anti-Virus are registered trademarks of Sophos Ltd. and Sophos Group. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.

The information contained in the Security Threat Report is for general information purposes only. It's provided by Sophos and SophosLabs and Naked Security. While we keep the information up to date and correct, we make no representations or warranties of any kind, express or implied, about the completeness, accuracy, reliability, suitability or availability with respect to the website or the information, products, services, or related graphics contained in this document for any purpose. Any reliance you place on such information is therefore strictly at your own risk.

The Sophos logo, consisting of the word "SOPHOS" in a bold, blue, sans-serif typeface.