

TOP TIPS FOR SAFER AND MORE SECURE ONLINE EXPERIENCES IN 2011

Cybercrime is a persistent fixture in the threat landscape. This undeniable fact is one of the key takeaways from last year. With its fair share of highs and lows, 2010 left an indelible mark on the security industry and consequently defined what the playing field will be like in 2011. Taking heed of the lessons that threat incidents left behind in 2010, we put together a recommended list of resolutions that users should follow to become better prepared for the year ahead. The threat landscape may be unpredictable at times but, for the most part, staying secure merely requires discipline. Find out what you need to stop, continue, and start doing starting today.

Lessons from 2010 Set the Pace for 2011

It became apparent in 2010 that one-dimensional threats were quickly fading into the background. The use of multicomponent threats that were harder to mitigate became the new norm. Threats today arrive via several attack vectors—spam, malicious URLs, file downloads, and vulnerability exploits—and may affect multiple platforms. When multiple vectors are used in a single attack, threat mitigation becomes even more difficult to do.



• If 2009 paved the way for some of the most persistent malware families and if 2010 was dubbed the “Year of the Toolkit,” users should expect no less in 2011.

If the recent year taught us anything, it is the fact that threats are not merely recurrent. It is that cybercrime is a work in progress that undergoes constant improvements. If 2009 paved the way for some of the most persistent malware families and if 2010 was dubbed the “Year of the Toolkit,” users should expect no less in 2011. Security experts believe that by using proven techniques in combination with newfound cybercrime tactics, cybercriminals are bound to have an even more profitable 2011.

Armed with this knowledge, users are encouraged to begin taking proactive steps toward creating a more secure online environment for themselves. As indicated in the “[Trend Micro Threat Predictions for 2011](#)” article, users should expect malware campaigns that will add a new spin to tried-and-tested social engineering techniques. From more targeted attacks to the evolving use of vulnerability exploits, users are bound to encounter even more dangerous threats. To serve as a quick guide, here are some of the top online activities that users should stop, continue, and start doing this year to become better prepared for what cybercriminals have in store for them.



1. Spammers are bound to keep the spam coming.

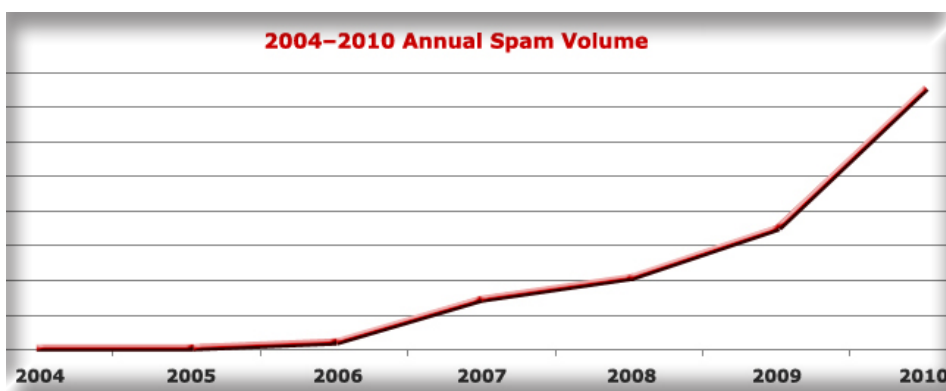
Stop opening email messages from unknown senders.

A review of the spam campaigns in 2010 revealed that while spammers remained active, no major changes **were seen in terms of the tactics they used**. Nonetheless, the fact remained that spammers continued to actively pursue their goals and to **send out spam for various purposes**.



Top tips for safer and more secure online experiences in 2011:

- Spammers are bound to keep the spam coming.
- Malicious URLs only lead to trouble.
- Not all file downloads are created equal.
- Mobile threats are now a fact of life.
- Vulnerabilities and exploits are evolving.



Continue verifying the authenticity of email messages.

By strictly avoiding opening messages from unknown senders, users can already prevent possible malicious payloads like information theft, malware infection, or, worse, both. It is thus a good practice to consciously check every email message that arrives in your inbox. For instance, an effective anti-phishing tactic involves mousing over an embedded link or image in an unverified email message then checking if the URL that appears on the lower left-hand corner of the browser window is legitimate or not. Scrutinize promotions and conduct your own research to verify seemingly legitimate offers received via email as well.

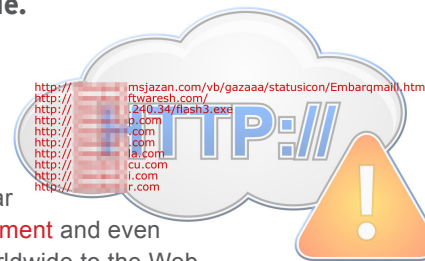
Start using email verification tools.

Since entirely relying on one's judgment may not always prove effective, utilizing tools designed to make email verification easier is the best bet. Most security software already provide this particular service by regularly scanning the email messages that a user receives. Nonetheless, installing **a browser plug-in** that is designed to determine an email message's legitimacy is a good idea to further keep cybercriminals at bay.

2. Malicious URLs only lead to trouble.

Stop clicking unverified links.

People are naturally curious and this fact is not lost on cybercriminals. In fact, this explains why a lot of attacks utilize popular keywords such as **Apple's iPad announcement** and even the "mystery keyword" that sent users worldwide to the Web for answers.



Users may encounter unverified links in spam and on websites. These links are, however, even more dangerous when found in social networking sites where users are more likely to let their defenses down, thinking they are in the company of friends. What most people fail to realize is that cybercriminals may just be using their friends to get to them. In sum, stop clicking suspicious-looking URLs, particularly those that include random characters.

Continue the practice of going back to the source.

As has repeatedly been said, one of the easiest ways to avoid infections via URL downloads is to go back to the source. Instead of recklessly clicking links that come up on search engine results pages, it is still far safer to directly access reliable sites and conduct searches from there. To check the legitimacy of search results, read their overview to ensure that these provide sensible descriptions.

The use of URL shorteners that effectively obfuscated malicious links likewise became widespread. To avoid being redirected to malicious sites, it is a good practice to verify the full versions of shortened links before going on a clicking spree.

Start brushing up on the concept of social engineering.

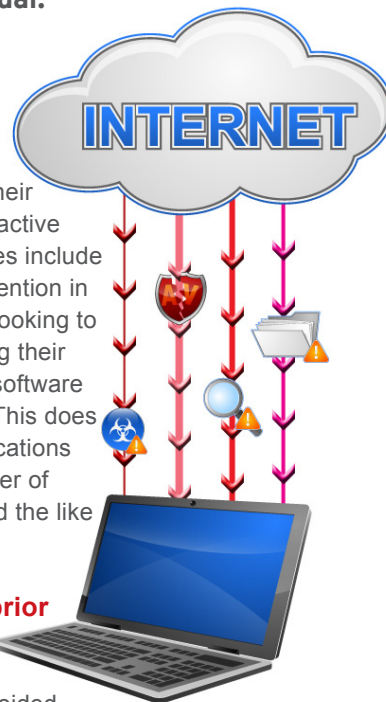
Possibly the most widely used cybercrime technique these days is social engineering. This includes the use of popular topics and of easily accessible channels like social networking sites to reach out to potential victims. By knowing exactly what they need to deal with, users will be better prepared to face the threats that cybercriminals may have in store for them this year.

► In a social engineering attack, an attacker uses human interaction (social skills) to obtain or compromise information about an organization or its computer systems.

3. Not all file downloads are created equal.

Stop downloading files from unsafe sources.

While it is already common for users to unknowingly download malicious files onto their systems, there are times when they play an active role in the infection process. Typical examples include spammed messages that require user intervention in downloading attached files. Similarly, users looking to save a few bucks sometimes end up infecting their systems by downloading and installing free software like **fake hard drive diagnostic applications**. This does not, however, mean that **free tools** and applications no longer exist these days. It's all just a matter of finding reliable sources like *SourceForge* and the like and of avoiding shady sites.



Continue the habit of scanning files prior to downloading.

If downloading files cannot be completely avoided, conducting file scans prior to doing so is the next best option. Using a **reliable security software** to scan files before downloading and opening or executing them adds an important layer of protection that can prevent possible infection.

Start reading end-user license agreements (EULAs).

License agreements are generally long and time-consuming to read. Unfortunately, taking time out to actually understand these can help users become more aware of what they are getting themselves into. Sometimes, in the process of downloading and installing software, other programs may be downloaded onto systems without the users' knowledge unless they actually read through entire EULAs.

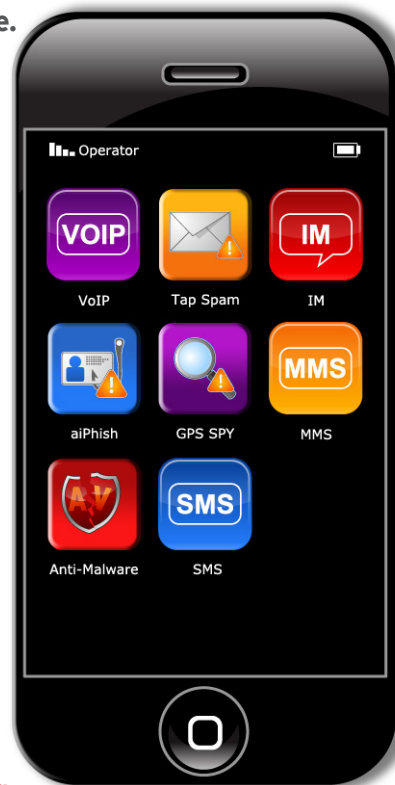
To steer clear of malicious file downloads in 2011:

- Stop downloading files from unsafe sources.
- Continue the habit of scanning files prior to downloading.
- Start reading EULAs.

4. Mobile threats are now a fact of life.

Stop unsecure mobile browsing.

Mobile devices have long been included in the list of cybercrime targets, most probably due to the considerable increase in their use. In fact, as many as six out of 10 American adults go online wirelessly using a laptop or any other mobile device. Recent technological developments likewise enabled seamless integration between traditional desktops and mobile devices. Users can literally browse the Web on the go, widening the playing field for malicious users who are on the constant lookout for new ways to proliferate their wares. Unfortunately, not all users realize that most of the threats they face online using traditional devices such as phishing attacks are the same threats that can hound their mobile experiences.



Mobile device use allows users to literally browse the Web on the go, widening the playing field for malicious users who are on the constant lookout for new ways to proliferate their wares.

Continue following mobile browsing best practices.

The mobile devices of today come with built-in security features like allowing the use of password locks and having the choice to turn bluetooth and other connectivity options on and off, as necessary. Users should take advantage of most, if not all, of these features to ensure their online safety as well as the security of the data stored in their mobile devices.

Just as security software use is important for desktops, users are also advised to take the same precautionary measures when browsing the Web via mobile devices. It is a good practice to be selective when downloading and installing mobile apps since these are also being used by cybercriminals in some attacks.

Users are also encouraged to browse sites or pages protected by Secure Sockets Layer (SSL) protocols if such an option is available via their mobile devices. Instead of logging in to banking and even social networking sites like Facebook using *http://*, they can opt to use *https://* to ensure an additional layer of defense against malicious attacks.

Start paying closer attention to the little details.

Since mobile devices generally vary in size and capability, there are certain cases wherein Web browsing can be more challenging than enjoyable. For instance, screen sizes dictate limitations in terms of browsing experience. This is crucial particularly when it comes to ensuring security. As one proof-of-concept (POC) attack showed, some mobile browsers **can effectively cloak full URLs**, which may be used for phishing attacks. By learning to take notice of the little details, users may effectively prevent malicious mobile attacks from succeeding.

5. Vulnerabilities and exploits are evolving.

Stop using unlicensed software.

Software piracy has become a pressing issue that has yet to be resolved. According to a **Business Software Alliance (BSA) study**, the forces driving piracy include the increasing sophistication of online criminals leveraging the Internet and other new distribution means. Furthermore, pirated software typically come from people with questionable ethics and whose skills include disassembling and cracking software. These same people can thus just as easily embed malware in pirated applications.



To stay protected against vulnerability exploit attacks in 2011:

- Stop using unlicensed software.
- Continue downloading regular software updates.
- Start brushing up on your vulnerability and exploit know-how.

Apart from the obvious copyright issues and possible malware infections surrounding the use of pirated software, another critical security problem has to do with the lack of updates.

Software vendors regularly patch and update their software to fix holes that may be used by attackers to penetrate unwitting users' systems. Apart from the usual vulnerability exploits targeting OSs and Internet-exposed services such as Web browsers, third-party applications **are also a favorite target**. As such, software updates are critical to ensure that systems stay safe from exploits.

Continue downloading regular software updates.

Once the good habit of downloading updates is in place, it's all a matter of keeping it. Often, users get prompts to download software updates but there are times when they ignore these. After all, the need to restart one's system in the middle of an important task can be quite discouraging. However, continued discipline is essential to stay safe and secure from threats.

Start brushing up on your vulnerability and exploit know-how.

In 2010, thousands of vulnerabilities were recorded by the National Vulnerability Database (NVD). This year, security experts expect an increase in the number of exploits for alternative OSs, programs, and Web browsers. As such, it will pay to invest more time in learning the ins and outs of vulnerabilities and exploits. This is admittedly tricky territory but once users get a good grasp of the concepts behind these, they would be better equipped to deal with future attacks. The *TrendLabs Malware Blog*, for one, is a good source of information on notable exploit attacks that users should be wary of.

Even security experts can only make presumptions as to what kinds of threat we can expect this year. In addition to emerging technologies and their accessibility, cybercriminals also dictate the pace at which the threat landscape evolves. This does not mean, however, that the security industry is incapable of creating the necessary protective measures to keep users safe. Likewise, users are fully capable of using the available resources to their full advantage in order to make their own online experiences safer and more secure in 2011.

By keeping these tips in mind, users stand a greater chance of surviving the year ahead unscathed. Cybercriminals will always try to find new ways to penetrate systems and to tear down the protective walls that security experts continuously put up. However, with the right mindset and the proper implementation of protective measures, users can just as easily arm themselves against malicious attacks.

** Please help us improve our reports by taking our quick survey.*

References:

- Aaron Smith. (July 7, 2010). *Pew Internet*. "Mobile Access 2010." <http://www.pewinternet.org/Reports/2010/Mobile-Access-2010.aspx> (Retrieved January 2011).
- Abhishek Bhuyan. (December 22, 2010). *TrendLabs Malware Blog*. "2010 in Review: The Vulnerability Landscape." <http://blog.trendmicro.com/2010-in-review-the-vulnerability-landscape/> (Retrieved January 2011).
- Bernadette Irinco. (August 17, 2010). *TrendLabs Malware Blog*. "Malicious Android App Spies on User's Location." <http://blog.trendmicro.com/malicious-android-app-spies-on-users-location/> (Retrieved January 2011).
- Business Software Alliance. (May 2010). "Seventh Annual BSA/IDC Global Software '09 Piracy Study." http://portal.bsa.org/globalpiracy2009/studies/09_Piracy_Study_Report_A4_final_111010.pdf (Retrieved January 2011).
- Carolyn Guevarra. (January 5, 2011). *TrendWatch*. "2010 Threats: The Good, the Bad, and the Ugly." http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/72_2010_threats_-_the_good__the_bad__and_the_ugly__010511_.pdf (Retrieved January 2011).

• Cybercriminals will always try to find new ways to penetrate systems and to tear down the protective walls that security experts continuously put up. However, with the right mindset and the proper implementation of protective measures, users can just as easily arm themselves against malicious attacks.

- Carolyn Guevarra. (January 27, 2010). *TrendLabs Malware Blog*. "FAKEAV Gets First Dibs in Profits from Apple iPad." <http://blog.trendmicro.com/fakeav-gets-first-dibs-in-profits-from-apple-ipad/> (Retrieved January 2011).
- David Sancho. (September 16, 2010). *TrendLabs Malware Blog*. "How Cybercriminals Hide Behind Multiple Web Layers." <http://blog.trendmicro.com/how-spammers-hide-behind-multiple-web-layers/> (Retrieved January 2011).
- David Sancho. (August 11, 2010). *TrendLabs Malware Blog*. "What Is 'Aixirivali Andorra' Anyway?" <http://blog.trendmicro.com/what-is-aixirivali-andorra-anyway/> (Retrieved January 2011).
- Jamz Yaneza. (December 9, 2010). *TrendLabs Malware Blog*. "FakeDiagnostics, Another Spin on FAKEAV." <http://blog.trendmicro.com/fakediagnostics-another-spin-on-fakeav/#more-30639> (Retrieved January 2011).
- Jonathan Leopando. (November 30, 2010). *TrendLabs Malware Blog*. "Mobile UI Spoofing—Another Reason for Smart Surfing." <http://blog.trendmicro.com/mobile-ui-spoofing%E2%80%93another-reason-for-smart-surfing/> (Retrieved January 2011).
- Maria Manly. (December 28, 2010). *TrendLabs Malware Blog*. "2010 in Review: Same Old Spammers." <http://blog.trendmicro.com/2010-in-review-same-old-spammers/> (Retrieved January 2011).
- Mindi McDowell. (October 22, 2009). *US-CERT*. "National Cyber Alert System: Cybersecurity Tip ST04-014—Avoiding Social Engineering and Phishing Attacks." <http://www.us-cert.gov/cas/tips/ST04-014.html> (Retrieved January 2011).
- Search Engine Journal. (January 28, 2010). *SEJ*. "How to Unshorten Any URL." <http://www.searchenginejournal.com/how-to-unshorten-any-url/16662/> (Retrieved January 2011).
- TrendLabs. (2009). *TrendWatch*. "2009's Most Persistent Malware Threats." http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/2009s_most_persistent_malware_threats__march_2010_.pdf (Retrieved January 2011).
- Trend Micro, Incorporated. (December 9, 2010). *TrendWatch*. "Trend Micro Threat Predictions for 2011." http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/trend_micro_2011_threat_predictions.pdf (Retrieved January 2011).