Prevent 11 types of hard-to-detect security crimes

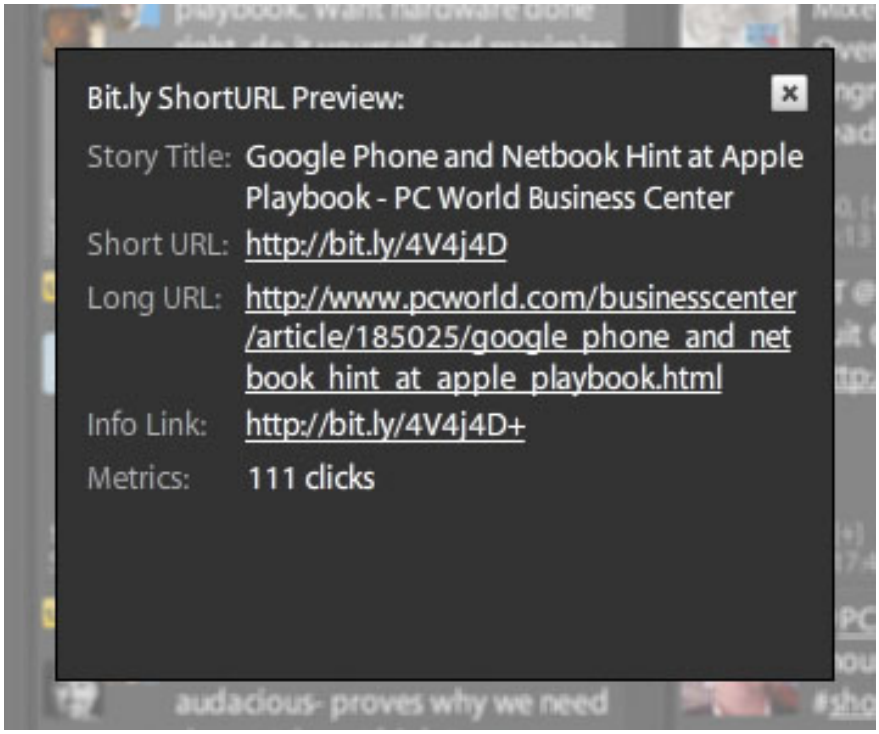
Antivirus software and firewalls are sometimes not enough to ensure you are safe. This is a way to help you avoid hidden attacks as well as attempts with bad intrigue

Network administration **- Antivirus software and firewalls are sometimes not enough to ensure you are safe. This is the way to distract hidden attacks as well as attempts with bad intrigue to steal user data.**

Indeed in the information society as it is today, there are many anti-virus software and firewalls created to protect users' computers from being safe. However, that is not enough, the cybercrime attack techniques are becoming more sophisticated and often preceded by the protection techniques contained in security software. So what do users have to do to avoid these sophisticated attacks? In this article, we provide you with 11 forms of the most malicious and most sophisticated attacks recently, along with tips to help you avoid or reduce the impact of these attacks.

1. The URL shortens

Most tweets and lots of other messages have links shortened by services like Bit.ly, Tr.im and Goo.gl. These URL aliases are indeed very useful, but they are also potentially risky: Because the URLs do not provide a destination destination, attackers can exploit them to send you malicious code pages.



Using Twitter client: Programs like TweetDeck contain options within their settings page to pre-display shortened URLs. When this feature is enabled, if you click on the shortened URL inside a tweet, you will see a screen appear, which will display the title of the landing page as well as the complete URL and number of others. Click on that link. With this information, you can make the right decision about whether to click on the link and visit that website.

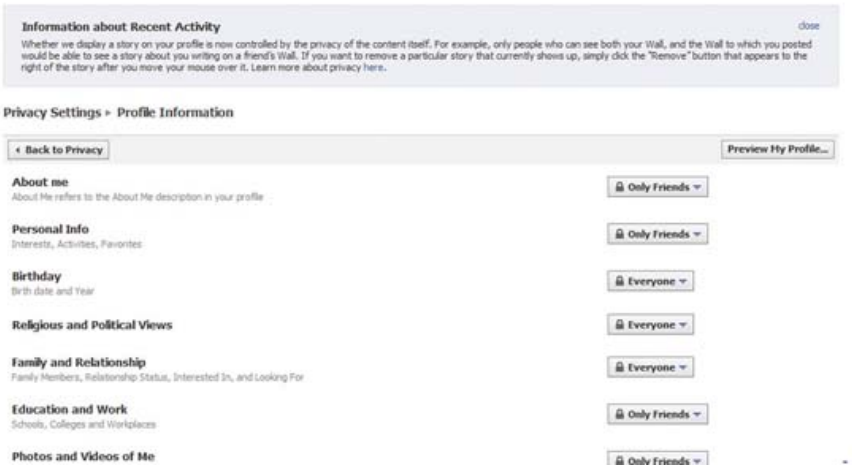
URL-preview plug-in settings: Some browser plug-ins and services can perform the same preview function as above. When you create a shortened address with the TinyURL service (for example), you can create a preview version so that the recipient can see the destination they will access before clicking. Conversely, if you're wondering about accessing the TinyURL link, you can enable its preview service to see the complete URL. To make the TinyURL preview work, you need to enable cookies in your browser.

ExpandMyURL and LongURLPlease, both provide browser or applet plug-ins that verify the safety of a complete URL behind shortened links from all known URL shortening services. However, instead of changing the shortened links to complete URLs, ExpandMyURL checks the landing pages in the background and marks the green for short-written URLs if they are harmless URLs.

Google, Goo.gl URL shortening service, also provides security by automatically scanning the destination URL to detect and identify malicious websites, and then alert users when shortened URLs can be harmful for users. However, Goo.gl has limitations that it only works with other Google products and services.

2. Harvest data from your Profile

Some personal data that you share on social networks, such as the school you studied in high school, the place of birth or the birth date, often resembles the same entries used in 'confidential' questions for banks and websites. If an attacker obtains this information, they can access your most sensitive accounts.



Check security settings on Facebook : After registering an account on Facebook, click on the menu bar and select *Privacy Settings.*

This setting will allow you to choose who can view your personal information. You can hide your details with everyone and only allow your network members to view them, or you can open the door and allow people to view your information. me In addition, you can set the privacy level for each component for your profile - such as birth date, religion and political views, photos you post or status updates.

Do not accept all friend requests from strangers : Over time, you will receive friend requests from someone you don't know. If you need to protect your personal information, then you should not accept these requests.

Be cautious when sharing : It is necessary to consider removing valuable information, such as birth dates and hometowns, from your profile. You should also consider carefully before joining and fun phrases of Facebook - these questions seem innocent and quite interesting but it is also the clue that criminals can exploit.

3. Impersonate social networks

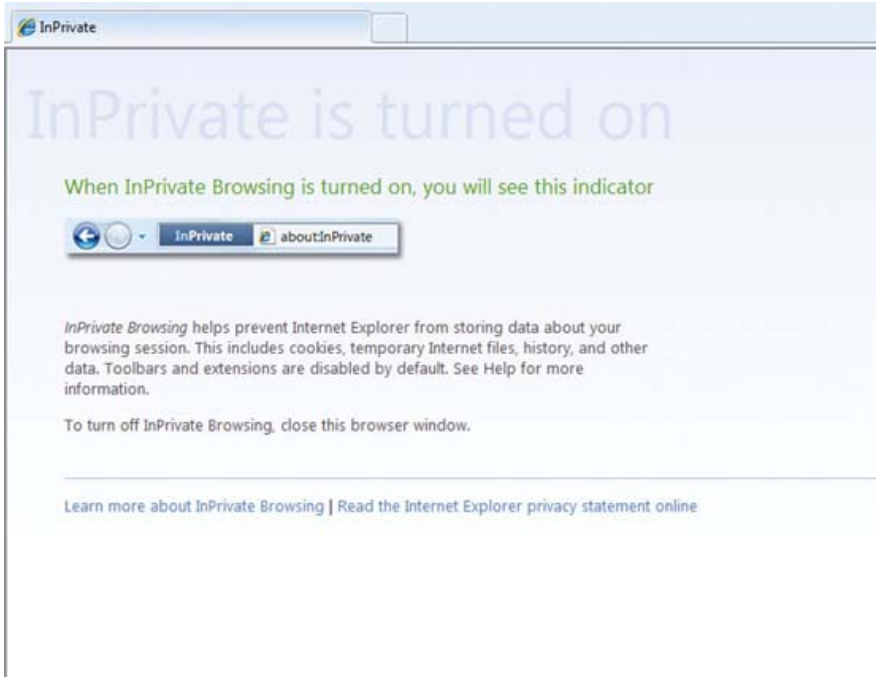
Whether you connect with someone who is authentic and trustworthy on Facebook, LinkedIn, Twitter, or other social networks. But the danger is still stalking you because attackers can still take control of this person's online personal information and exploit that trust.

Be wary of bad scams who impersonate in the name of friends : An attacker can hijack the control of one of someone's online network accounts among your close friends via malware, or carefully. Some tricks, then use these stolen accounts to spam you, steal your personal data, or even cheat to get your money. When attackers hijack control of a group member account of your friends (this member cannot access their account at this time), they can send you notifications urging, pleading like: ' *Help me , I'm in HCM and lose my wallet. You can send me some money to buy a plane ticket to Hanoi* . ' Or they may incite you to click on certain links, thereby infecting your computer or compromising your personal account.

4. Snooping on the web

Today, entertainment, sales or some social organizations are online, so Internet users can be traced. The book you have read, the movie you have rented, the person you are dealing with, the shopping items you buy or other details are forming a personal data warehouse for search engines, homes. advertising as well as anyone who wants to snoop on your computer.

Working with companies you trust : You need to know the privacy policies of the websites and services you interact with so you can trust that you can protect sensitive information. mine.



Use private browsing mode : Current browser versions such as Internet Explorer, Firefox, Safari and Chrome both offer private browsing mode. Features like InPrivate Browsing in IE 8, Private Browsing in Firefox 3.5 can ensure information such as site history, form data, searches, passwords and other information of the current session is no longer saved. on the browser cache or password protection when you turn off the browser.

Page 3: Fake software

5. Fake software

Sure you know a lot about fake attacks, impostors can use decoys like an email designed as if it was sent from a bank or a financial institution to hook users. Fake software often comes with fake attacks to trick you into installing bad antivirus software on your computer by 'warning' that your computer may be infected with a virus .

Don't touch the bait : Stop and think. For example, if you have not installed any security software on your computer, then where does this notification come from? If you already have a security utility to identify and lock malicious software, why does it tell you to buy or download additional software to fix the infection that your computer is having? Be familiar with the warnings of the security software you are using so that you can easily identify the fake warning.

No panic : You should have malware protection available on your side. If you don't have security and security software, you need to worry about your computer, then scan your system with Trend Micro, HouseCall, or free online malware scanners. Run Microsoft's Malicious Software Removal Tool. When you complete your scan, whether you discover a problem or not, you should find yourself an anti-malware application and install it on your computer to protect your computer in the future.

Browser upgrade : Such fake notifications will prompt you to access a number of dishonest websites, which can make your system infiltrate to a worse extent. The current versions of most web browsers and many Internet

security suites have built-in anti-phishing protection, to warn you about fake sites. However, you need to keep in mind that the databases that these filters use are updated regularly to identify fake sites, but they are still not secure enough, so you need to pay attention. to the URLs you may visit. To help you make a faster decision, Internet Explorer 8 and Chrome both bold the original domain name in the URL so you can know whether the domain name that you will access is trusted.

6. Trojan Horse

Some attacks will send spam messages to your mobile phone to assume that they are provided from certain network providers or financial institutions. These Trojan horse messages may lead you directly to the malicious site or may require permission to install an upgrade that can change the settings on the phone, which allows an attacker to capture the username. , password and other sensitive information from your device.

Get access to sources that contain updates and news : If you receive a message sent from a trusted source, however, it directs you to install or upgrade a software, or initialize it. During the installation process or have permissions requirements to continue, then exit the application to read the message immediately and contact the service provider's customer service department to verify the information. Is that valid or not?

You can receive a lot of emails due to requests from companies that you still have contact with, but reputable companies will not send you links and updates due to requests. by email. Similarly, reputable companies will not send unsolicited messages to mobile devices to ask you to install an upgrade, or download some new software.

Attackers often tend to trick you into passing your trust in wireless service providers as well as financial institutions. Therefore, you should not blindly accept software upgrades or download applications to your mobile phone.

Page 4: Losing laptop, data is revealed

7. Losing laptop, data is revealed

The portable capabilities of laptops and mobile phones make them convenient, but this also means that these devices are easy to lose or steal. If your laptop or mobile phone falls into the wrong hands, these people can access the sensitive data you have stored in it.

Data encryption : You can use a utility like Microsoft's BitLocker to encrypt data. However, BitLocker is only available for Windows Vista and Windows 7, even in Ultimate and Enterprise versions only in these two operating systems (also available in Windows Server 2008).

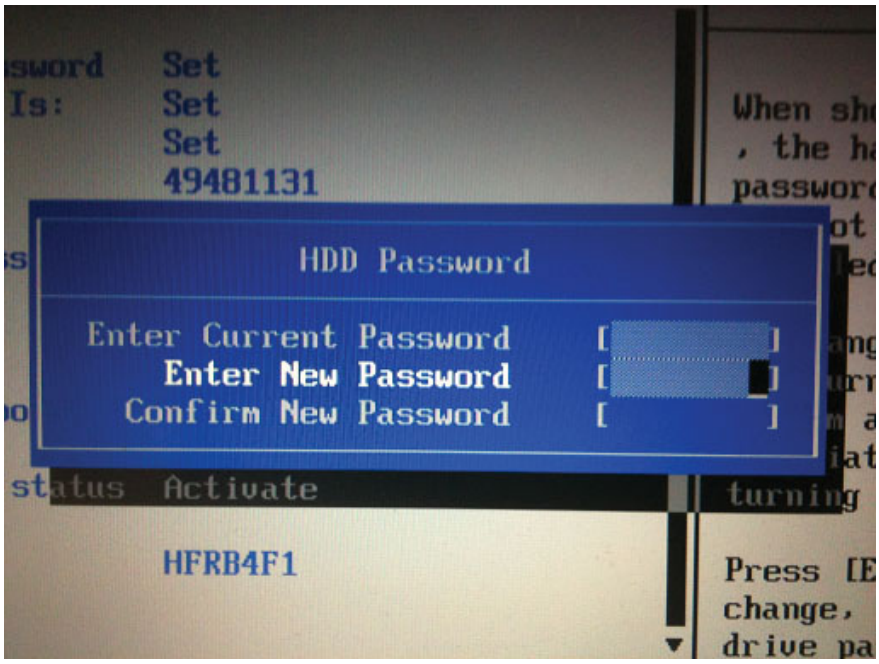
However, BitLocker is not the only program you can use. In addition to this program, it is possible to use other encryption programs, such as TrueCrypt (provided free under open source registration) to protect your data against bad guys.

However, the data encryption is like a double-edged sword. The biggest problem is making sure you always remember the encryption key. If you lose your encryption key, then you will see how hard it is to encode it again.

Use strong passwords : If encryption seems more complicated than what it is worth, you can use strong passwords to protect your computer. The longer the password, the better, the more characters will make

unlocking more time consuming. You should also mix multiple symbols by replacing numbers and special characters for letters. For example, instead of using an original ' **tenban** ' password, you can use ' **tenb @ n** '. It's a cluster that you can easily remember, but this passphrase contains many components that will make cracking more difficult.

There should also be a secure password to log in to your user account even if only you use that computer. Note, although strong passwords can be difficult to guess, you can still be attacked the other way: An attacker who owns your computer can find many ways to bypass this protection.



Lock your BIOS : By executing a BIOS password or hard drive password (or both), you can be sure that no one can start your computer. With the BIOS in the systems, the initial boot screen that the computer displays usually indicates which keys you need to press to access the BIOS settings.

When accessing the BIOS settings page, look for security settings. These settings may vary between brands, but it can be said that the BIOS settings are quite simple.

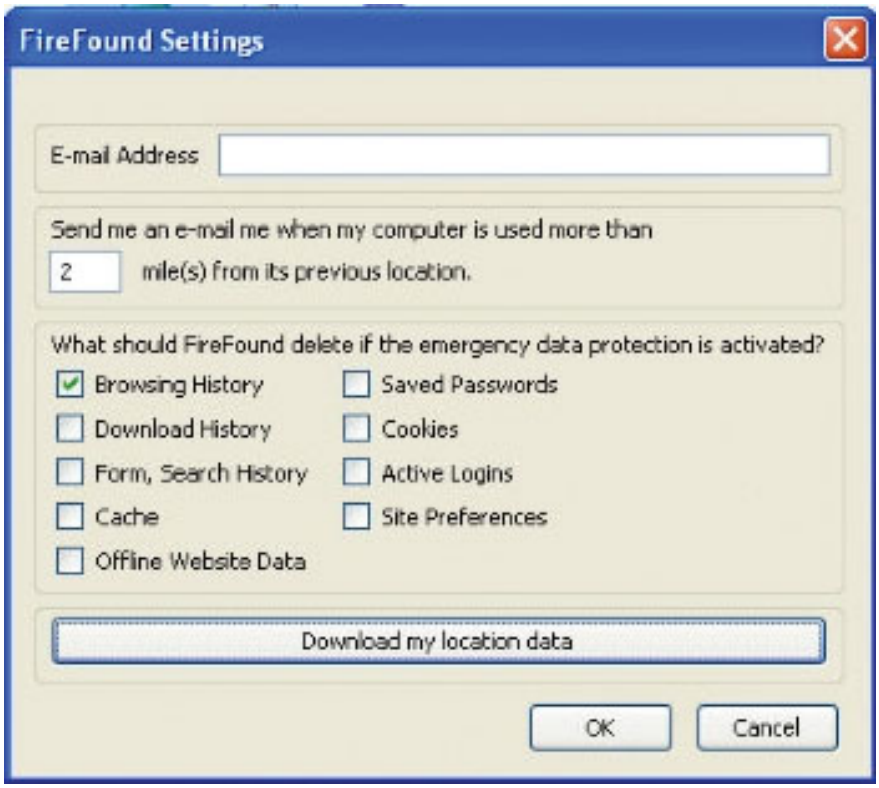
You can set up a master password to prevent others from starting your computer or changing BIOS settings. This option has different names, but usually they are still called ' *Administrator password* ' or ' *Supervisor password* '. If you want, you can also set the hard drive password, which will prevent access to the hard drive until the correct password is entered.

There may be many ways to bypass these passwords, but setting up the correct passwords will create an additional layer of security and may hinder all attacks including attacks. most professional.

Use recovery service : If your device is lost or stolen you often want to regain it; however, if you cannot find your hardware, at least you should delete the data on it. Some vendors, such as HP and Dell, offer both.

Both Notebook and Restore tracing services from HP and Dell are based on Absolute Software's Computrace technique. When you report a laptop that is protected by one of these lost or stolen services, a small application

running in the background in that computer will wait until the computer is connected to the network. Internet and contact the testing center to exchange location information to search for computers. If you can't find a lost or stolen laptop that protects this service, or if the data on the system is very sensitive, these services can remotely erase all data on the computer. there.



Although less comprehensive, free utilities like add-on FireFound for Firefox also have similar features. You can configure FireFound so that it can automatically delete passwords, browser logs and cookies.

Mobile phones can also keep a significant amount of sensitive data. However, users can use **Find My iPhone** service, part of MobileMe service of Apple and **Mobile Defense** for Android mobile phones to perform traces and delete data remotely. Both MobileMe and Mobile Defense can use the GPS capabilities included in the phones to indicate the device's current location and forward that information to you.

Page 5: Fake Wi-Fi Hotspot

8. Fake Wi-Fi Hotspots

Free Wi-Fi networks may appear more and more. However, attackers sometimes set up unique Wi-Fi networks to lure users to connect. When someone connects to this fake wireless network, they can capture their computer traffic and collect the sensitive information you sent, such as username and password.

Network name verification : If you want to connect to the Internet at a certain café or public location, find out the vendor's network SSID. SSID is the name of the wireless network; it is broadcast to your computer so that it can detect the network and is the name that appears on your list of available networks.

The SSID for a network at a McDonald's restaurant might be " **mickeyds** ". Phishers can set up a fake wireless router in the vicinity of McDonald's location and set up an SSID of " **mcdwifi** " or " **mickeyds2** ". Your computer will then display both of these networks in the list - even if the fake network has a stronger signal strength and appears above the list. Make sure you are smart enough to recognize the official network.

When in doubt, don't trust any network to open. Most wireless networks are not encrypted - and so are unprotected networks. This means that data transmitted between computers and wireless routers is vulnerable to eavesdropping or being stolen by another component that appears within the wireless network. Unless you have a secure connection, such as a VPN (virtual private network) connection to the network at the office, you should avoid using public Wi-Fi networks to log sensitive accounts (such as email or bank account); limited, only use the Internet in public places to read newspapers and check for news on weather forecasts and traffic reports.

9. Weak Wi-Fi security

If you are cautious, you can secure your wireless network with a password to prevent strangers from accessing and using your Internet connection. However, password protection here may not be enough .

Use strong encryption : There are several types of Wi-Fi network encryption and there are some differences between them. WEP (Wired Equivalent Privacy) encryption is the most typical type of encryption and has been deployed on wireless networks. If you have set a WEP password for your Wi-Fi network, you have taken a step forward in protecting your network from being compromised.

However, WEP is still vulnerable to cracking: There are many tools that allow you to help an attacker crack your code and access your network in a matter of minutes. However, WEP is still very useful because most wireless attackers with bad intentions are not professional enough to be able to crack it, but to be safer you should use WPA (Wi-Fi). Protected Access) or WPA2. These two types of encryption can overcome WEP's weaknesses and provide stronger protection.

Log in to the router's console and look for wireless security settings. Here, enable encryption and select WPA or WPA2. Enter the password, save the settings and restart the router - you can now start surfing the web more safely.

10. Backup data is dangerous

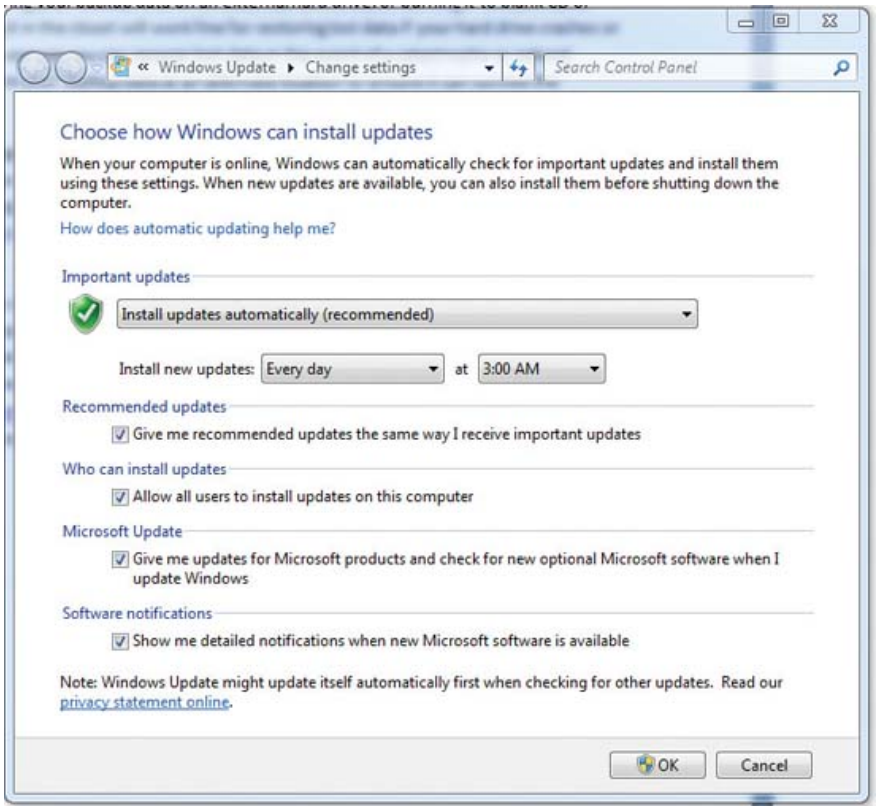
You may know that you should backup your data, especially files that cannot be replaced like family photos. However, while storing backups on an external hard drive or writing them to a CD or DVD for example and keeping them somewhere, it allows you to recover files easily if the hard drive fails or broken, but this method also creates a portable storage of sensitive data - and so is easy to lose or stolen.

Encrypt backup data : Need to use a backup utility that allows you to protect your data by encryption or at least a password, to prevent unauthorized access. If you want a more secure step, put your backup files on an encrypted USB external device like Seagate Maxtor BlackArmor. You can also choose external drives with fingerprint scanners like Apricorn Aegis Bio or LaCie d2 Safe.

Using online backup service : If you like, you can use online storage solution like Microsoft Windows Live SkyDrive, this service gives you 25GB of free storage, data security for you by love need username and password to access. However, copying 25GB of data and updating it regularly through SkyDrive can take a long time and create a cumbersome process. For a small fee, you can use another service like Mozy, which includes tools that automate the backup process and make sure your data is backed up regularly.

11. Software is not patched (not just Windows)

Microsoft products have long been favorite addresses for malware, but the company has entered and fought these attacks by searching for weak links in the security chain. Today, third-party software such as Adobe Reader is also a means for an attacker to take advantage of it to hack into your computer.



Install all security updates : You should install both a firewall and an anti-malware utility to protect your system, but one of the simplest - and most effective - ways to protect you before the attack is a timely update of your operating system and applications.

Attackers have found that there are some applications of third parties such as Adobe Reader and Adobe Flash that have some weaknesses that can help them exploit to break into your computer. To ensure that you can combat these threats, you can use programs like Secunia Personal Software Inspector to scan your system, identify vulnerable applications, and then install updates. necessary.

It is important to keep up with the new errors that appear for the applications you are using, and apply the appropriate patches immediately.Http://antivirus.about.com/ may be a trusted address so you can collect such information. You can also check sites like http://vil.nai.com/vil/default.aspx to find the latest news about attacks.

Although attacks on third-party applications may face less resistance, some attackers still do not give up on Microsoft products. Windows users need to enable Automatic Updates (or Windows Update) and set up to download and install automatic security updates. Automatic upgrades will keep your operating system as well as Microsoft software such as Internet Explorer and Office applications always have the latest patches.

Page 6: 5 confidentiality

5 security confessions

Sometimes users who are easily misguided about their security status are safe and these are 5 of those misconceptions:

1. I have nothing needed for an attacker to look at .

Ordinary users assume that data on their computers is only valuable to them and not valuable to others, so they do not have a protection plan and are not worried about the computer being hacked. public. However, this is completely wrong. First, instead of stealing data, an attacker often wants to control your own computer so that they can use a compromised computer to spread malware or spam. Th? hai, b?n có th? ngh? r?ng máy tính c?a mình không có d? li?u quan tr?ng ho?c nh?y c?m nh?ng k? t?n công có th? s? d?ng các thông tin d??ng nh? t?m th??ng, ch?ng h?n nh? tên, ??a ch?, ngày sinh ?? ?ánh c?p s? nh?n d?ng c?a b?n. Th? ba, h?u h?t các t?n công ?? u ???c th?c hi?n t? ??ng, tìm ra và th?a hi?p t?t c? các h? th?ng có l? h?ng; chúng không phân bi?t d?a trên giá tr ? c?a m?c tiêu.

2. Tôi ?ã cài ??t ph?n m?m ch?ng virus do ?ó máy tính c?a tôi hoàn toàn an toàn .

Ph?n m?m ch?ng virus qu? th?c r?t c?n thi?t, nó là m?t kh?i ??u t?t cho máy tính c?a b?n, tuy nhiên ch? có ph?n m?m này thì hoàn toàn ch?a ??. M?t s? s?n ph?m ch?ng virus không có kh? n?ng phát hi?n và khóa ch?n spam, các c? g?ng gi? m?o, spyware hay các t?n công mã ??c. Th?m chí ngay c? khi b?n có m?t ph?n m?m b?o m?t khá toàn di?n ?? b?o v? ch?ng l?i các nhi?u m?i ?e d?a ngoài virus thì b?n v?n ph?i nâng c?p nó m?t cách th??ng xuyên: Các ph?n m?m mã ??c m?i ???c phát hi?n hàng ngày và vi?c b?o v? ch?ng l?i mã ??c ch? t?t n?u ???c c?p nh?t th??ng xuyên. C?n l?u ý r?ng các hãng b?o m?t c?ng c?n có th?i gian ?? b? sung thêm s? b?o m?t ??i v?i m? t t?n công m?i ???c phát hi?n, chính vì v?y ph?n m?m ch?ng mã ??c s? không b?o ??m b?n ???c an toàn trong các t?n công m?i hay t?n công zero-day.

3. B?o m?t ch? là v?n ?? khi s? d?ng Windows.

Các s?n ph?m c?a Microsoft luôn là m?c tiêu c?a các t?n công b?o m?t các v?n ?? có liên quan t?i b?o m?t trong nhi?u n?m, tuy nhiên ?i?u ?ó không có ngh?a r?ng các h? ?i?u hành khác và các ?ng d?ng khác là ??ng ngoài. M ?c dù các s?n ph?m c?a Microsoft bi t?n công nhi?u nh?ng Linux và Mac OS X c?ng ?ã cho th?y c?ng có các l? h?ng và c?ng b? t?n công. Khi các h? ?i?u hành và các trình duy?t khác có ???c s? l??ng ng??i dùng ?ông ??o, khi ?ó ch?c ch?n chúng c?ng s? tr? thành các m?c tiêu t?n công. Thêm vào ?ó, các t?n công c?ng ?ang nh?m ??n các s?n ph?m c?a các hãng th? ba ngoài các h? ?i?u hành, ch?ng h?n nh? Adobe Reader.

4. Router c?a tôi có t??ng l?a, do ?ó máy tính c?a tôi ???c b?o v? .

T??ng l?a r?t t?t cho vi?c khóa các truy c?p ng?u nhiên hay trái phép vào m?ng c?a b?n, máy tính ???c ??t sau t ??ng l?a khi k?t n?i Internet, do ?ó nó s? ???c t??ng l?a b?o v? tr??c m?t lo?t các t?n công; tuy nhiên các k? t?n công v?n có th? vòng tránh và qua m?t ???c t??ng l?a ?? t?n công b?n thông qua các c?ng truy?n t?i d? li?u m? r? ng. M?c ??nh, t??ng l?a s? khóa l?u l??ng thông th??ng ch?ng h?n nh? d? li?u web và email, tuy nhiên ch? có m? t s? ít ng??i dùng có th? ?ánh giá các thi?t l?p t??ng l?a và quy?t ??nh xem l?u l??ng nào c?n ch?n và l?u l??ng nào cho phép ?i qua. Thêm vào ?ó, nhi?u t?n công ngày nay d?a trên web ho?c ???c t? ch?c t? m?t t?n công gi? m?o có th? l?a b?n truy c?p vào các website mã ??c; t??ng l?a không th? b?o v? b?n trong nh?ng t?n công ki?u này.

5. Tôi ch? truy c?p các website có danh ti?ng, do ?ó tôi hoàn toàn không có gì ph?i lo ng?i v? v?n ?? b?o m?t

.

?ây là m?t nh?n th?c hoàn toàn sai l?m vì các website n?i ti?ng nh? Apple, CNN, eBay, Microsoft, Yahoo, hay th ?m chí c? FBI c?ng ??u ?ã b? th?a hi?p b?i các t?n công cross-site scripting nh?m thu th?p thông tin v? ng??i dùng ho?c cài ??t ph?n m?m mã ??c lên máy tính c?a ng??i truy c?p.

Các ngu?n b?o m?t khác

Nhi?u website và d?ch v? trên m?ng có th? giúp b?n h?c h?i v? các m?i ?e d?a b?o m?t máy tính hay có th? phân tích máy tính c?a b?n ?? b?o ??m nó ???c s?ch s? và an toàn.

Hoax Encyclopedia: About.com có m?t c? s? d? li?u khá toàn di?n v? email và các th? do virus gi? m?o. Tr??c khi b?n chuy?n ti?p c?nh báo kh?n c?p sang gia ?ình ho?c b?n bè c?a mình, hãy ki?m tra nó trên danh sách này tr ??c.

McAfee Virus Information Library: McAfee duy trì m?t danh sách ch?a các t?n công malware, g?m có các thông tin chi ti?t v? cách chúng tr?i r?ng nh? th? nào và cách b?n có th? b?o v? máy tính c?a mình ra sao.

Microsoft Consumer Security Support Center: Trong trang này, b?n có th? tìm th?y các gi?i pháp cho các v?n ?? b?o m?t nói chung, c?ng nh? các liên k?t ??n các thông tin và tài nguyên khác cho các s?n ph?m b?o m?t c?a Microsoft.

Microsoft Malicious Software Removal Tool: Công c? này ???c thi?t k? ?? quét và g? b? các t?n công hi?n hành. Trình quét c?a nó khá nh? và nhanh h?n nhi?u so v?i m?t trình quét antimalware hoàn ch?nh, tuy nhiên nó ch? có th? nh?n d?ng ra các t?n công khó ch?u. Microsoft th??ng phát hành phiên b?n m?i cho các công c?– cùng v?i ?ó là các b?n vá b?o m?t – vào ngày th? Ba trong tu?n th? hai hàng tháng.

Microsoft Security Essentials: ?ng d?ng antivirus mi?n phí này cung c?p cho b?n s? b?o v? th?i gian th?c cho các máy tính Windows tr??c virus, worms, spyware hay các ph?n m?m mã ??c khác.

PhishTank: M?t d? án c?ng ??ng, PhishTank là m?t c? s? d? li?u ch?a các site gi? m?o. B?n có th? tìm ki?m c? s ? d? li?u ?? nh?n d?ng các site gi? m?o, có th? b? sung vào danh sách này b?t c? site gi? m?o m?i nào mà b?n b?t g?p.

Trend Micro Housecall: D?ch v? HouseCall c?a Trend Micro có th? quét tr?c tuy?n máy tính c?a b?n ?? phát hi ?n và g? b? viruses, worms hay các ph?n m?m mã ??c khác ?ang c? trú trên nó.