Users Beware:
10 Tips for Avoiding Online Security Traps

Summary

ThreatTrack Security has compiled these 10 tips to help users avoid common online threats.

IT professionals know the damage that malware can cause, but everyday users are often unaware of the security threats lurking on the web, in their email and on their smartphones.

Even the best malware defense can be rendered useless due to careless user behavior. To defend against data breaches, it's critical that users understand the security threats and cybercrime tactics they face.

User training is a best practice used by organizations of all sizes to bolster their cyber defense. jmrDesign LLC is pleased to share the following information provided by ThreatTrack Security in order to help educate users to understand the critical role they play in preventing data breaches.

Although the tips offered in this article focus on user behavior, it is also important to have an effective security solution in place on user systems. jmrDesign LLC offers Managed Anti-Virus / Anti-Malware services using the VIPRE technology provided by ThreatTrack Security.

200,000+
NEW MALWARE THREATS
ARE CREATED
EVERY DAY

High risk user behavior is now considered to be the number one threat to cybersecurity.

1. Understand Cybercrime and Malware

Malware is malicious software code developed by cybercriminals to infect PCs, networks and mobile devices for the purpose of gaining access to and extracting sensitive data, typically for financial gain. There are more than 200,000 new malware threats created every day[1], and nearly 70% of data breaches involve malware.[2]

The days of malware being created and released by hackers for fun and gaining notoriety are long gone. Today, malware fuels a global multi-billion dollar cybercrime economy.

You are their #1 target. Whether you're using a PC at home or at work, you are just a tool for cybercriminals to gain access to the data they want to steal or the systems they want to hijack.

To defend yourself and your organization's data, it is important to understand that malware writers are becoming very adept at creating threats that evade detection by traditional security solutions. Don't assume you can let your guard down or behave in a riskier manner because your PC at home or work is defended by antivirus, email security, firewall or other cyber defenses. One wrong click and your PC is infected, and data is at risk.

Some malware types – like **viruses** and **Trojans** – are tools for breaking into your PC, while others – like **worms**, **spyware** and **key loggers** – are all about snooping through a PC or network looking for particular systems to compromise and data to steal. Many data breaches involve multiple kinds of malware in a staged attack that progresses over time. It's critical to understand that one infected PC may seem like a small problem, but it can lead to big trouble for the organization.

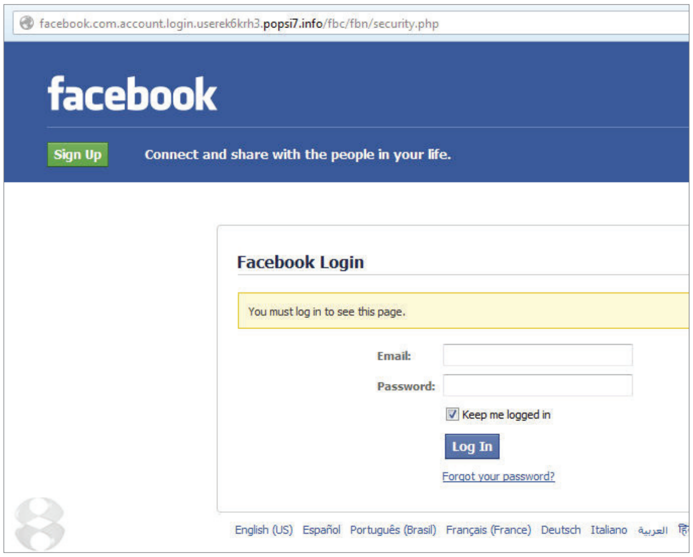
Still other malware – like **bots** or **bot nets** – are all about hijacking PCs to steal computing resources to launch other cyber-attacks. Instead of paying for legitimate IT infrastructure and equipment to start a spam campaign, scammers often secretly use a network of infected PCs around the world to distribute malicious email without users ever knowing.

Tip: Don't underestimate how clever cybercriminals have become. Their tricks are extremely effective at luring users to open infected files, click on malicious links, unwillingly share malware with colleagues, and to freely divulge sensitive data. They understand how we behave online, and they know exactly what to do to infect us. Knowing the types of tricks and traps they use is the first step to defending yourself and the organization from malware.

2. Be Difficult to Catch

Believe it or not, one of the most common ways that cybercriminals gain access to sensitive data is by tricking users into divulging information we ordinarily wouldn't share with anyone.

It's called **phishing**, and it often involves using **social engineering** tactics to trick users into thinking they have been contacted by a service they know and trust – like a bank, online retailer, airline or social media platform – typically via a fraudulent email requesting that a user disclose sensitive information like passwords, credit card details and even social security numbers.



facebook.com.account.login.userek6krh3.popsi7.info/fbc/fbn/security.php

Connect and share with the people in your life.

You must log in to see this page.

Does this Facebook login screen look real to you? It's not. It was part of a phishing campaign to steal passwords.

Social engineering refers to the practice of creating deceptive attacks based on what is known about the targeted user. For example, cybercriminals scour users' social media accounts like Facebook and LinkedIn to create phishing emails that look and read real enough to trick users into responding to fraudulent requests to change passwords, confirm payment options or divulge other personal information.

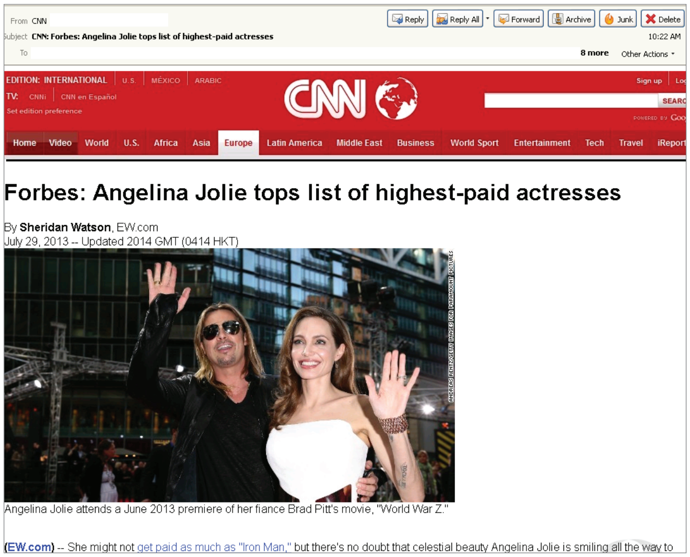
Phishing emails and the websites they link to look like the real thing and can be difficult to identify as malicious right away. URLs or web addresses also look legitimate. And since many people re-use the same password, a user's login credentials for a bank account is often the same one they use to log on to the network at work every day. This enables cybercriminals to access the work network as if they were you.

Tip: Always keep in mind that most of the services you use will never request that you share personal information directly via email. Moreover, the majority of time you are contacted to reset a password or confirm any changes to your account will be initiated by an action you take. In the event you receive an unsolicited email (even if it's an alarming warning to reset a password), it is best to assume it is malicious. Do not click any links. Contact the service provider or check their website by entering the URL you always use.

3. Resist Your Curiosity

Malicious spam remains a major threat to many organizations. These aren't those annoying marketing emails we're tired of deleting from our inboxes all day long. Think of malicious spam as a precursor to phishing, employing similar tricks of deception – stealing logos and designs from well-respected brands – to trick users into clicking malicious links or downloading infected files. Malicious spam could even come from an email address spoofed (manipulated) to appear as if it is from someone within your organization. But one click of the mouse to open an infected Word document or PDF, and your PC may be infected.

Just about any type of malware can be delivered via malicious spam. Cybercriminals use spam as a "shotgun" tactic to spread their malware as wide as possible. Often these emails are disguised as shipping confirmation notices, alarming notices from banks, tantalizing photos, mortgage scams, fake news alerts and more – anything to raise our curiosity and get us to open an email and click an attachment or link that only leads to trouble.



Subject CNN: Forbes: Angelina Jolie tops list of highest-paid actresses

Forbes: Angelina Jolie tops list of highest-paid actresses

By **Sheridan Watson**, EW.com
July 29, 2013 -- Updated 2014 GMT (0414 HKT)

Angelina Jolie attends a June 2013 premiere of her fiance Brad Pitt's movie, "World War Z."

(EW.com) -- She might not get paid as much as "Iron Man," but there's no doubt that celestial beauty Angelina Jolie is smiling all the way to

This malicious spam used the CNN logo and the public's curiosity about Angelina Jolie to deliver malware.

Tip: Always be wary of any email you receive that is out of the ordinary or you did not request. Spam can look very real, but avoid the temptation to click without thinking. Also, be aware that just because you're at work and protected by security solutions, malicious spam can still slip through. Best course of action, if you think it's spam, delete it.

4. Browse with Care

Another favorite trick of cybercriminals is **poisoned search results** or **black hat SEO**. This is another way malware writers use our curiosity against us by exploiting high-profile events like a celebrity scandal, new tech gadget or major events like the Olympics, a royal birth, an election or sports championship. Cybercriminals know what people are searching for online and talking about via social media, and they use that against us.

While search engines like Google are very good at protecting us from these threats, cybercriminals are quick to stand up entire websites within hours of sensational news breaking, claiming video and pics, but only delivering malware to visitors. It may take Google a few hours to identify and remove these sites from its search results, but in that time plenty of users can be infected.

Tip: Get your celebrity gossip and news from trusted sites only. Always be careful what you're searching for and what sites you visit on your lunch hour. Again, don't assume you're protected because work has better security than your home PC. Threats – especially newly created threats – can still slip through.

5. Don't be Exploited

Two types of malware known as **exploits** and **Zero-day attacks** refer to cybercriminals taking advantage of vulnerabilities in the software products we use every day. These include operating systems like Windows, web browsers like Chrome, Internet Explorer and Firefox, and a wide range of popular applications like Adobe Flash and Reader, Java and Skype.

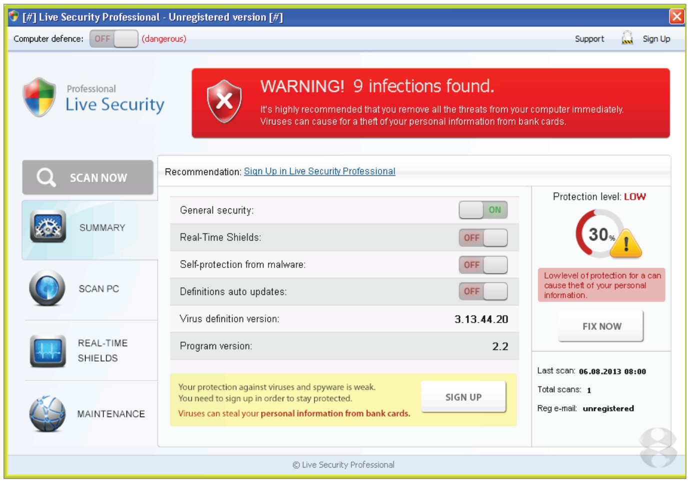
Malware writers invest a lot of time and energy searching for faulty software code they can exploit and use as a backdoor into your PC to deliver malware for any number of malicious purposes. Zero-day attacks are named as they are because at the time of their discovery there is no fix for the vulnerability they are exploiting, leaving software companies scrambling to release updates within a few days, which is plenty of time for cybercriminals to spread malware.

Tip: The best defense against malware exploits is to always update software programs to the latest available versions. When a message appears on your screen to update a trusted software application, do it. Chances are good the software developer is correcting an issue that may have serious security implications. If your organization uses an automated patching solution, these updates should be deployed automatically. However, be mindful of Zero-day alerts from IT, which may instruct you to avoid using certain programs when a threat is identified.

6. Watch for Malware in Disguise

Cybercriminals know that users are concerned about security and often employ messages and pop-up screens that appear to be legit programs on your PC requesting updates. Clicking on these links can lead to downloading malware and installing **rogue applications**.

These rogues may claim to be antivirus products or system cleaning programs. Some even claim to be from the FBI. They look authentic, but they are designed to infect your PC to extort money from you, or to install additional malware on your computer.



[#] Live Security Professional - Unregistered version [#]

Computer defence: OFF (dangerous)

WARNING! 9 infections found.

It's highly recommended that you remove all the threats from your computer immediately. Viruses can cause for a theft of your personal information from bank cards.

Recommendation: Sign Up in Live Security Professional

General security: ON

Real-Time Shields: OFF

Self-protection from malware: OFF

Definitions auto updates: OFF

Virus definition version: 3.13.44.20

Program version: 2.2

Protection level: LOW

30%

Lowlevel of protection for a can cause theft of your personal information.

Your protection against viruses and spyware is weak.
You need to sign up in order to stay protected.
Viruses can steal your personal information from bank cards.

Last scan: 06.08.2013 08:00

Total scans: 1

Reg e-mail: unregistered

© Live Security Professional

This very legit-looking rogue is actually malware called Reveton, which uses scare tactics to lock PCs and demand payment from users to purchase false protection.

Tip: If you see a warning claiming your PC is infected, don't click anything. Contact IT. Don't take the chance.

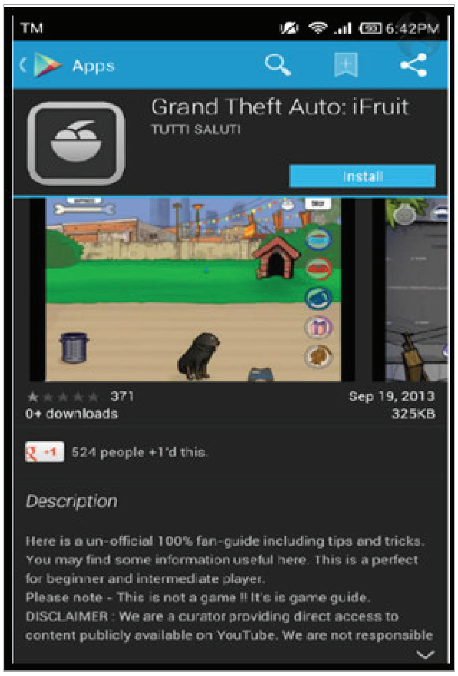
7. Back it Up

There is a family of malware known as **ransomware**, and just like the name implies, these malicious programs take your PC hostage. By clicking on the wrong link in an email or by visiting an infected website, your PC can fall victim to malware that demands payment to be removed, or even worse large sums of money to regain access to your files. Hijacking users' PCs and encrypting files so they are no longer accessible is an increasingly popular tool in the bad guys' arsenal.

Tip: Avoid ransomware by being safe online, but be prepared for the worst and back up all critical files your business or operation can't do without. And since ransomware is often delivered via malware exploits, keep your system patched and software up to date.

8. Stay Safe While Mobile

Malware is no longer limited to just PCs. With the rise of mobile devices and their proliferation in the workplace, malware writers have switched tactics to take advantage of these inviting targets. Malicious Android and iOS apps can cause all sorts of headaches – from running up international text charges to stealing personal data and passwords to transmitting infections to other devices, like your PC.



Grand Theft Auto: iFruit

TUTTI SALUTI

371

0+ downloads

Sep 19, 2013

325KB

524 people +1'd this.

Description

Here is a un-official 100% fan-guide including tips and tricks. You may find some information useful here. This is a perfect for beginner and intermediate player.
Please note - This is not a game !! It's is game guide.
DISCLAIMER : We are a curator providing direct access to content publicly available on YouTube. We are not responsible

This game wasn't even available for Android when this malicious rogue look-alike was making the rounds, frustrating users and redirecting them to unwanted and potentially harmful content.

Tip: Don't think that your Android or iOS device is safe from threats. Mobile malware is the fastest growing segment of malware. When downloading apps, only download from trusted sources (Google Play and Apple's App Store) and only choose apps from trusted developers. Moreover, install a trusted security app onto your mobile device.

9. Don't be a Carrier

Just like people can spread the flu or a cold to colleagues, users can spread malware infections to their work PC and network. Two common ways this happens is by sharing files between a work and home PC that may not be as secure or is used by other family members who do not practice safe online habits.

Users may work on an infected document on their home PC and email it to their work computer or upload to the cloud where other users may access it, getting infected themselves.

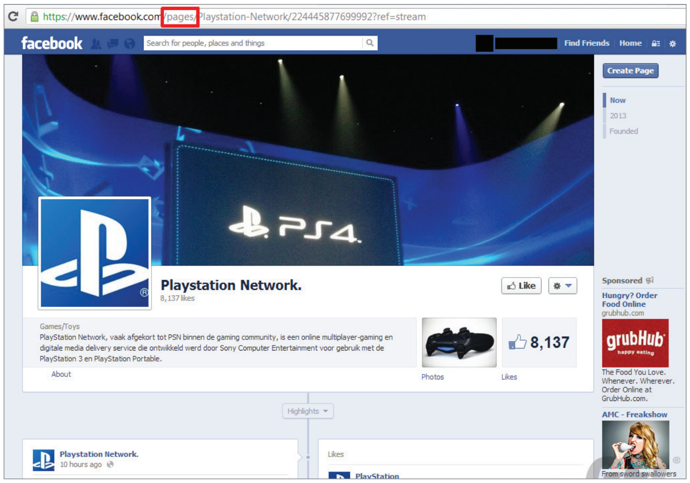
Moreover, removable storage devices, like USB sticks and external hard drives are often shared among users. Malware writers know this and create threats that are designed to stealthily move from these devices to PCs.

Tip: Only connect your PC to trusted devices and scan all USB drives with your antivirus software before opening any files. Be mindful of who is using a home PC if you are opening work documents on it. Always ask if you completely trust the surfing habits of your 13-year-old son or daughter.

10. Avoid Friendly Threats

Security threats on social media continue to grow exponentially. Shortened links are effective tools to hide malicious URLs, and threats tied to compelling images and videos shared on Facebook can spread quickly among friends.

Cybercriminals can quickly set up fake accounts and profiles to spread malware, typically employing the same social engineering tactics they've perfected. Moreover, cybercriminals can hijack your profiles and accounts to spread malware under your name to people you're connected to.



https://www.facebook.com/pages/Playstation-Network/224445877699992?ref=stream

Games/Toys

PlayStation Network, vaak afgekort tot PSN binnen de gaming community, is een online multiplayer-gaming en digitale media delivery service die ontwikkeld werd door Sony Computer Entertainment voor gebruik met de PlayStation 3 en PlayStation Portable.

The Food You Love. Whenever. Wherever. Order Online at GrubHub.com.

Scammers set up this fraudulent page to capitalize on PlayStation fans' anticipation of a new product launch, pointing them to spam and other unwanted content.

Tip: Be careful what you click on Facebook, Twitter, LinkedIn and other popular social channels. Only share and click on posts from trusted sources, and be mindful that it's possible your friends are sharing malware. Also, use different passwords for all your accounts, so if one is compromised the others are still secure.

Stay Safe

By adopting these 10 tips, users can do their part to protect their network from data breaches, protecting critical data, safeguarding customer privacy and defending your organization's reputation.

About ThreatTrack Security Inc.

ThreatTrack Security specializes in helping organizations identify and stop Advanced Persistent Threats (APTs), targeted attacks and other sophisticated malware designed to evade the traditional cyber defenses deployed by enterprises and government agencies around the world. The company develops advanced cybersecurity solutions that **Expose**, **Analyze** and **Eliminate** the latest malicious threats, including its ThreatSecure advanced threat detection and remediation platform, ThreatAnalyzer malware behavioral analysis sandbox, ThreatIQ real-time threat intelligence service, and VIPRE business antivirus endpoint protection.

jmrDesign
Data Driven IT Solutions LLC

To learn more about jmrDesign LLC
call 717-451-4707 or visit
www.jmrDesign.net.

To learn more about ThreatTrack Security
call +1-855-885-5566 or visit
www.ThreatTrackSecurity.com.

ThreatTrack SECURITY

[1] Verizon; 2013 Data Breach Investigations Report
[2] ThreatTrack Security Labs

The information and content in this document is provided for informational purposes only and is provided "as is" with no warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose, and non-infringement. ThreatTrack Security, Inc is not liable for any damages, including any consequential damages, of any kind that may result from the use of this document. The information is obtained from publicly available sources. Though reasonable effort has been made to ensure the accuracy of the data provided, ThreatTrack Security, Inc makes no claim, promise or guarantee about the completeness, accuracy, recency or adequacy of information and is not responsible for misprints, out-of-date information, or errors. ThreatTrack Security, Inc makes no warranty, express or implied, and assumes no legal liability or responsibility for the accuracy or completeness of any information contained in this document. If you believe there are any factual errors in this document, please contact us and we will review your concerns as soon as practical.