

# How to Secure Your Multiple Online Accounts





You have multiple accounts all over the Web whether you're a casual browser, a social media guru or a tech-savvy webmaster. We conducted a study and found out that an average user juggles at least ten online accounts. This is no surprise, considering that the Internet offers quite a number of convenient services like email, online shopping and banking, and more.

But how does someone with ten or more accounts ensure that each of them is secure? With more and more web-based services opening up, how does the same user manage his/her account security?

This e-guide provides users with knowledge on how to safeguard and protect multiple online accounts no matter how many they are.





Why Should I Be  
Concerned?

If there's anything netizens should be concerned about, it's the risk of private data ending up in the wrong hands. Here are some of the risks you could be subjecting yourself to:

- **Identity theft.** Cybercriminals can use your credentials for their own transactions or dealings. These could lead to unintended payments for products or services. Identity theft is so common that it happens every 3 seconds. Also, according to our latest study, 1 in 3 people know someone who's been a victim of identity theft.
- **Financial theft.** Cybercriminals have been known to infiltrate and drain victim's bank accounts. In 2010 alone, more than US\$37 billion were stolen from 8.1 million adults in the United States through electronic theft.
- **Actual theft/burglary.** There is a potential risk of burglars using your online information to rob from your own home. Context clues may help criminals verify that you and your family are out of the house. A study revealed that 80% of robbers check victims' social networking accounts for planning heists.<sup>1</sup>
- **Reputation compromise.** Other people gaining access to your online accounts may lead to not so desirable consequences. They may send malicious messages to those in your contact list or post inappropriate material on your social networking profile. There is a good chance that other linked accounts could also end up being compromised.



1 <http://www.smartplanet.com/blog/science-scope/infographic-80-of-robbers-check-twitter-face-book-google-street-view/11082>



How Can I Protect My  
Online Accounts?

Fortunately, your accounts are protected at the outset of their creation, all thanks to the humble password. The digital equivalent of a key, the password has been protecting users since early computing days. As they are created by the user, they should be foolproof.<sup>2</sup>

Unfortunately, users tend to take passwords for granted.<sup>3</sup> Users often see passwords as something of a bothersome obstacle to their accessing their personal content.

Typical known passwords are very simple, derived from common names, abbreviations and sequential numbers (e.g., *monkey, password, 123456*). Common words from the dictionary are also often used.

Another pain point for users is keeping track of how many passwords they have and which password applies to which account. This is usually the reason behind reusing passwords.<sup>4</sup>

All of these unsafe habits can lead to account infiltration. Proper password creation and management, therefore, should be the primary concern.

---

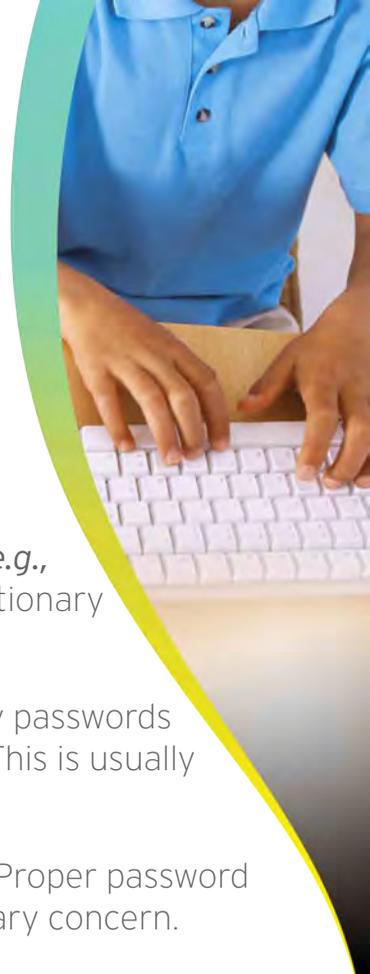
2 <http://blog.trendmicro.com/infographic-go-all-in-when-it-comes-to-password-security/>

3 <http://blog.trendmicro.com/the-trouble-with-passwords/>

4 <http://about-threats.trendmicro.com/us/webattack/131/Will+Your+Passwords+Pass+the+Test>

## BAD PASSWORD HABITS

- **33%** of users either save their passwords in a .DOC/.TXT file or write them down on paper.
- **10%** of users have a single password for all their accounts.





# 7 Practical Tips

- **Keep your password longer than 10 random characters.** It should also not be used for more than one account.
- **Be creative with your security answers.** Making them totally out of context to the security question. Some sites also allow you to create your own security questions.
- **Steer clear of phishing attacks.** Phishing is a cybercriminal's way of tricking you into providing your login details. Don't open suspicious messages or click links from unfamiliar sources.
- **Regularly patch or upgrade your software.** Info-stealing malware rely on software vulnerabilities in order to penetrate systems. This also applies to your mobile device.
- **Reduce your digital clutter.** Delete accounts you no longer need. This removes the link between your old and existing accounts.
- **Limit what you share on your social networking accounts.** You may be revealing too much about your private life which may be used against you.
- **Use a password manager.** *Trend Micro™ DirectPass™* keeps track of every password you have for every online account. It can automate and ease the complicated process of managing several passwords.

## **SECURE YOUR PASSWORD!**

- Keep your password longer than ten characters. The longer, the better.
- Replace letters with numbers and/or punctuation marks.
- Use a "passphrase" instead of a password. A three-word nonsensical phrase is ideal.
- Use nonconsecutive numbers. Avoid using significant dates like your birthday.
- Never reuse your passwords. Take the time to create one for each account you have.

## TREND MICRO™

Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global cloud security leader, creates a world safe for exchanging digital information with its Internet content security and threat management solutions for businesses and consumers. A pioneer in server security with over 20 years' experience, we deliver top-ranked client, server and cloud-based security that fits our customers' and partners' needs, stops new threats faster, and protects data in physical, virtualized and cloud environments. Powered by the industry-leading Trend Micro™ Smart Protection Network™ cloud computing security infrastructure, our products and services stop threats where they emerge—from the Internet. They are supported by 1,000+ threat intelligence experts around the globe.

## TRENDLABS<sup>SM</sup>

TrendLabs is a multinational research, development, and support center with an extensive regional presence committed to 24 x 7 threat surveillance, attack prevention, and timely and seamless solutions delivery. With more than 1,000 threat experts and support engineers deployed round-the-clock in labs located around the globe, TrendLabs enables Trend Micro to continuously monitor the threat landscape across the globe; deliver real-time data to detect, to preempt, and to eliminate threats; research on and analyze technologies to combat new threats; respond in real time to targeted threats; and help customers worldwide minimize damage, reduce costs, and ensure business continuity.



Securing Your Journey  
to the Cloud

