7 Password Security Tips to Keep You Safe Online

Identity theft is increasing online, but the security experts at Google have strategies to keep you safe.

By Kristen Sturt

Safety First

Think identity theft can't happen to you? Think again.

In 2012, the **Federal Trade Commission (http://ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2012.pdf)** reported more than 350,000 cases in the U.S. alone. About 54 percent of those reporting were older than 40, and collectively, they lost millions to benefits, credit card, and utilities fraud.

Those numbers are only growing, and that's why it's more important than ever to guard your personal information – especially online. We spoke to Google security spokesperson Nadja Blagojevic about ways to protect yourself, from creating dynamic and memorable passwords to how you should respond to suspicious emails. Read on for her tips.

1. Get creative with your passwords.

Forget **12345 (http://www.youtube.com/watch?v=_JNGI1dI-e8)**, your dog's name, and any words that make actual sense. Instead, try combining markedly different characters, which makes it harder for criminals to guess your password.

"We suggest that password be at least eight, if not more, characters. We also suggest that people use a mix of letters, but also numbers, and what we call special characters – the ampersand, etc," says Blagojevic.

2. Use different passwords for different

websites.

Good news: You created an airtight password!

Less-good news: You have to create many more, since it's a bad idea to use a single password for multiple websites.

Blagojevic has a great way of explaining it: "When you think about it, a password is really like a key to a website. When you use the same password for all your sites online, it's like you're using the same key for your car, your house, your mailbox. And when you lose that key, it means that someone can access all those things."

3. Write your passwords down on paper.

So, you've created a series of hard-to-guess passwords that virtually guarantee online security. How in the world do you remember them?

Three words: write them down.

It turns out, the odds of a crook finding those passwords, knowing what they're meant for, and using them successfully are very slim. "It's both intuitive and counterintuitive," says Blagojevic. "If you're worried you're making your password too long, it's okay to write it down and put it in your desk or wallet."

4. Look for multiple-step verification.

To ensure protection, some websites can ask for information in addition to a password. Sometimes, it's the answer to a security question of your own devising. Other times, it's a special code that's sent to your phone.

Google offers the latter option: "We have whole teams of engineers whose full-time job is to work on security and work on privacy at Google," says Blagojevic. "Two-step verification is a free Google tool that allows you to protect your Google account with more than just a password."

5. Don't share.

"The one thing we really encourage users is to think carefully before you share information," Blagojevic cautions. Trustworthy businesses will never ask you to hand over your personal data, and that includes your security codes. "If you receive an email asking you to share your password, it's probably a scam. If [an email] seems a little suspicious, take a minute and think about whether the request makes sense."

6. Report scams.

"If you see something that looks wrong, [don't] enter any information, and report that scam to the **Better Business Bureau (http://www.bbb.org/us/Dispute-Resolution-Services/Identity-Theft-Resources/)** or the **FTC (http://www.consumer.ftc.gov/features/feature-0014-identity-theft)**," says Blagojevic.

The **National Consumers League (http://www.nclnet.org/)** website has special sections dedicated to **Fraud (http://www.fraud.org/)** and **Identity Theft (http://www.nclnet.org/personal-finance/124-identity-theft/224-think-youve-been-a-victim-of-id-theft)**, where you can find more on reporting crimes and bringing lawbreakers to justice.

7. Move from Florida to South Dakota.

Sorry, sunbathers. According to the **FTC (http://ftc.gov/sentinel**

/reports/sentinel-annual-reports/sentinel-cy2012.pdf), identity theft is highest in the Sunshine State, where it occurs at almost twice the rate of any other state. In fact, 9 of the top 10 worst cities for ID theft are in Florida, with Miami leading the list.

South Dakotans, on the other hand, have the lowest ID theft rate in the country, followed closely by their neighbors in North Dakota. How do you feel about snow?

View Slideshow (javascript:void(0);)