



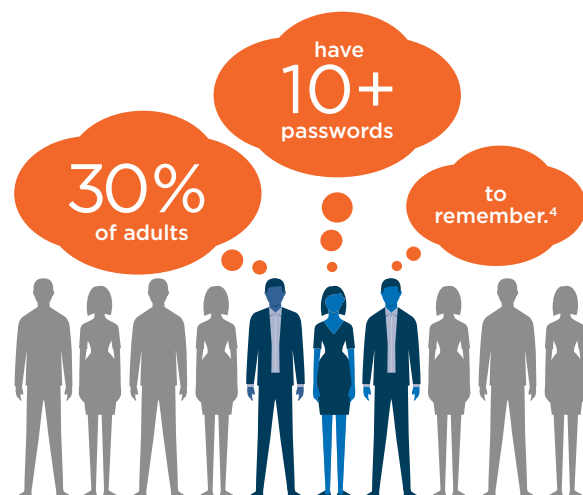
Protect what's yours

Together we can defend your data

Nearly three quarters of Americans have fallen victim to some type of cyber crime.¹ In recent years, an average of **4 in 10 people have received a notice that their personal information had been compromised**, had an account hacked and/or had a password stolen. Perhaps that's why 8 in 10 people say they are worried about their online security.²

Passwords pose problems

Almost every login requires a password: bank accounts, shopping accounts, smartphones, email access, etc. Most people have more passwords than they can keep track of, so they tend to choose simple, easy-to-remember ones; however, this makes it easy for cyber thieves as well.



It doesn't take long for a hacker's computer to guess a password³



— versus —



Fortunately, it can be easy to reduce your risk. Just turn over this page.

Protect your retirement account by creating your own online access first.

You might think that the best way to not get hacked would be to not create an online account in the first place. But hackers can be clever, especially if the payoff could be access to your money or personal information. Using information they can gather elsewhere, they attempt to create online accounts. Your best defense is to go on offense.

- Go to nationwide.com
- Select “Log In or Sign Up”
- Toggle “Retirement Plans”

In just minutes, you will establish a User Profile that will help reinforce the virtual firewall we’ve built to keep hackers out. In addition to creating strong passwords, to strengthen safeguards around all of the online accounts you have, consider these tips.

Be secure online

- **Vary usernames.** Your username is your “first password.” Every time you create a new online account, give yourself a new username.
- **Update software automatically.** This will help ensure your system gets the latest updates as soon as they’re released.
- **Enable screen locking on your devices.** Many devices offer security features which may allow you to remotely lock them or even erase all data if it is lost or stolen.
- **Log out and close your browsing windows.** Doing so reduces the possibility of unauthorized use of an already logged-on account.
- **Consider the information you share on social media sites.** Review the social media site’s privacy and security settings to control who can see your profile.

Shop carefully

- **Look for “https” in the web address.** “Https” is generally more secure than “http.” Avoid financial transactions on “http” sites.
- **Avoid public computers.** Thieves install keystroke tracking software on library or hotel lounge computers to steal usernames and passwords.
- **Know your surroundings.** Limit your use of financial apps when you’re where people can easily look over your shoulder and see your inputs or information.

Act fast if you’ve been hacked

- **Change your usernames and passwords for all sites and accounts you use,** especially sites which may contain financial and personal data.
- **Ask your financial institutions to look for fraudulent activity.** Many companies, including Nationwide, can set up alerting and monitoring on your account activity.



.....
For more tips, go to nationwide.com/protect
.....

¹ 4 Scary Hacking Statistics You Probably Didn’t Know About. (April 2016). Retrieved from <https://stellarbluetechologies.com/2016/08/4-scary-hacking-statistics-you-probably-didnt-know-about/>

² June 2015 Telesign Consumer Account Security Report: An International Study of Digital Security Concerns and Practices polled 2,000 consumers in the U.S. and the U.K.

³ The Problem with Passwords, Bloomberg Businessweek (January 2011)

⁴ Why Your Password is Hackerbait, Entrepreneur (January 2015)