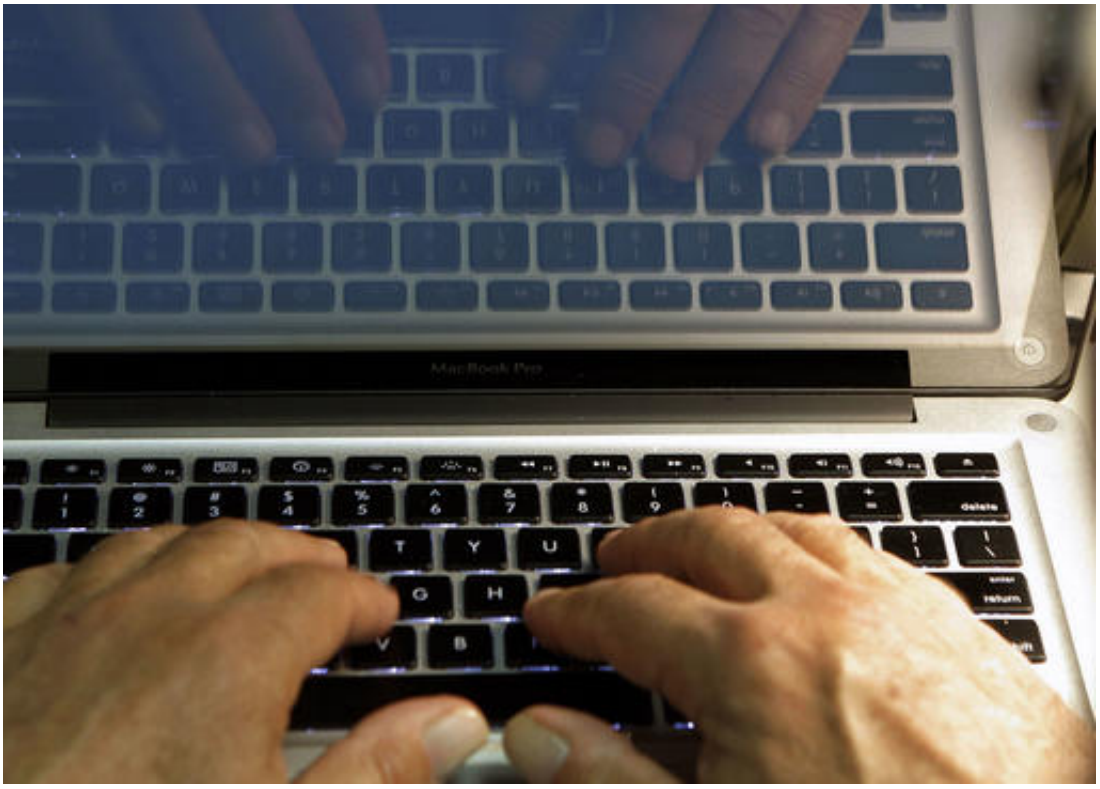
Zuckerberg hacking serves as reminder to change passwords

June 6 2016, by Bree Fowler



In this Feb. 27, 2013, file photo, hands type on a computer keyboard in Los Angeles. News that Facebook founder Mark Zuckerberg's rarely used Twitter, LinkedIn and Pinterest accounts were briefly compromised should serve as a reminder that we're all susceptible to hacking. (AP Photo/Damian Dovarganes, File)

Mark Zuckerberg can be hacked and so can you.

The Facebook founder's rarely used Twitter, LinkedIn and Pinterest accounts were briefly compromised on Sunday, serving as a reminder that everyone is susceptible to hacking.

Safeguards you could take include creating strong passwords and changing them frequently. Yes, all this is a pain, and it's not your fault that the tech industry couldn't grapple with the rise in security breaches. But if you do nothing, someone could break into your financial account or use your social media account to spew obnoxious or hateful messages. Think of how many friends you'll lose.

Here are six things you can do to stay safe.

___

PICK A GOOD PASSWORD

The more complicated and lengthy a password is, the harder it will be for hackers to guess.

Don't include your kids' names, birthdays or references to any other personal details. Hackers routinely troll Facebook and Twitter for clues to passwords like these. Obvious and default passwords such as "Password123" are also bad, as are words commonly found in dictionaries, as these are used in programs hackers have to automate guesses.

Long and random combinations of letters, numbers and other characters work best.

___

DON'T REUSE PASSWORDS

Avoid using the same password for multiple sites, so that a break of your school's PTA site wouldn't lead hackers to your online banking account.

You can make things easier on yourself by using a password-manager service such as LastPass or DashLane. They remember complex passwords for you—but you have to trust them. Last June, LastPass disclosed "suspicious activity" and told users to change their master passwords.

Some web browsers such as Apple's Safari and Google's Chrome also have built-in password managers. They work if you switch devices but not if you switch browsers.

___

NEW TOOTHBRUSH? NEW PASSWORD

It's important to change your password regularly, just as good physical hygiene calls for replacing your toothbrush every few months.

And don't be tempted to recycle an old one. The longer a password sits around, the more likely it is to fall into the wrong hands.

And if company announces that it's been hacked, change your password right away, even if it says your information wasn't compromised. Breaches are often worse than they first appear. LinkedIn recently disclosed that a 2012 breach affected 117 million accounts— not the 6.5 million previously thought.

___

MAKE IT HARDER

Multi-factor identification—which asks users to enter a second form of identification, such as a code texted to their phone—will provide additional protections at services that offer it.

Even if hackers manage to get your password to, say, Facebook, they still need your phone with the texted code. It's not as much of a pain as it seems, as services typically ask for this second code only when logging on from a new device or browser.

___

TAKE OUT THE TRASH

Delete or deactivate accounts you no longer use. Got a spam-filled Juno or AOL email account lying dormant? Maybe it's time to say goodbye.

Just last week, Myspace said a hacker has put up for sale login information for some accounts created before June 11, 2013.

If, like most people, you've moved on to greener social media pastures, permanently get rid of the ones you no longer use. This often can be done through your account settings—as long as you still have your password to sign in.

___

SOCIAL MEDIA CLEAN UP

And while we're on the subject of social media, make sure you restrict posts to just your actual friends. You can adjust that in the settings.

Some companies try to help their users with this. Facebook, for example, occasionally prompts its users to review who can see their personal

information and how strong their security settings are.

Nonetheless, assume that everyone everywhere can see what you're posting. Personal tidbits can not only help hackers crack easy passwords, they also can be used to answer supposedly personal questions to reset passwords.

More information: AP's tips on securing smartphones: apne.ws/1RWxo5o

AP's tips on avoiding phishing: goo.gl/NZTldV