

Lessons from Yahoo hack: Simple tips to safeguard your email

16 March 2017, by Mae Anderson



In this, Monday, Dec. 12, 2016, photo illustration, a woman types on her laptop, in Miami. Details from the Department of Justice indictment of Russian hackers on Wednesday, March 15, 2017, show that many people are still not taking routine precautions to safeguard their email accounts, and hackers are exploiting that. (AP Photo/Wilfredo Lee)

Details from the Department of Justice indictment of Russian hackers on Wednesday show that many people are still not taking routine precautions to safeguard their email accounts—and hackers are exploiting that.

The Russian hackers didn't have to work very hard to break into people's email accounts, even those belonging to government officials or powerful executives. Here's a look at a few simple ways to help safeguard your email account from hackers.

DON'T REUSE PASSWORDS

Many online break-ins result when people have reused a password across, say, their email, social and financial accounts. If it's compromised at any one of those services, the others are suddenly vulnerable.

One simple way to avoid this problem is to start with a base password you can remember, and then add on letters and numbers that reference where you're using it. If your base password is "greatsurfer2017" (which isn't particularly secure; more on that in a moment), you could make "greatsurfer2017Y" your Yahoo password, and "greatsurfer2017G" your Google password.

If you can't be bothered to do more, this is a base level of security that can help shield you from the most obvious threats. But it's still only a baby step.

PICK A STRONGER PASSWORD

You can make things harder for attackers by making your base password stronger. The more complicated and lengthy a password is, the harder it will be for hackers to guess.

The downside: Tougher passwords are also harder to remember. But there are some ways around that.

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.



This Jan. 14, 2015, file photo shows a sign outside Yahoo's headquarters in Sunnyvale, Calif. In an indictment Wednesday, March 15, 2017, announcing charges against four Russians, U.S. officials describe how Russian hackers working with Russian intelligence officials broke into Yahoo's network, stole information on Yahoo user accounts and ultimately gained entry into other services used by individuals they were targeting. (AP Photo/Marcio Jose Sanchez, File)

You can make your own strong passwords with randomly capitalized nonsense words interspersed with numbers and characters—like, say, "giLLy31!florp." (Just don't use that one now that it's appeared in this story.) So long as you're making up the words yourself, these are difficult for hackers to crack—and they're easier to remember than you might think, though you might want to practice them a few times.

HAVE YOUR PASSWORDS MANAGED FOR YOU

Of course, you can make things easier on yourself by using a password-manager service such as LastPass or DashLane, which keep track of multiple complex passwords for you. Some web browsers such as Apple's Safari and Google's Chrome also have built-in password managers; these work if you switch devices, but not if you switch browsers.

After you create a strong password for your password manager, it can create random passwords for your other accounts—and will

remember them for you as well.

"It's more secure and it makes your life easier," said Jamie Winterton, director of strategy at the Global Security Initiative at Arizona State University.

MULTIFACTOR AUTHENTICATION IS A MUST

The next line of defense is two- or multifactor authentication, which asks users to enter a second form of identification, such as a code texted to their phone, when they log in. It's now commonplace for many email and social media accounts. That way, even if hackers manage to get your password they still need your phone with the texted code.

"Having another way for that account to say 'Hey, is that really you?', and give veto authority is really important," Winterton said.

KEYWORDS MATTER

According to the indictment, the Russian hackers searched email accounts for keywords like "passwords" to find people's passwords for other accounts. They also searched for "credit card" "visa," among other terms. So think twice before you use common key words that can serve as a road map to sensitive information for hackers. And don't save passwords in old emails.

"There's not one single thing out there that can keep you perfectly safe," Winterton said. "But there are a lot of different things out there that can keep you almost perfectly safe."

© 2017 The Associated Press. All rights reserved.

APA citation: Lessons from Yahoo hack: Simple tips to safeguard your email (2017, March 16) retrieved 21 September 2021 from <https://phys.org/news/2017-03-elude-russian-hackers-decent-password.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.