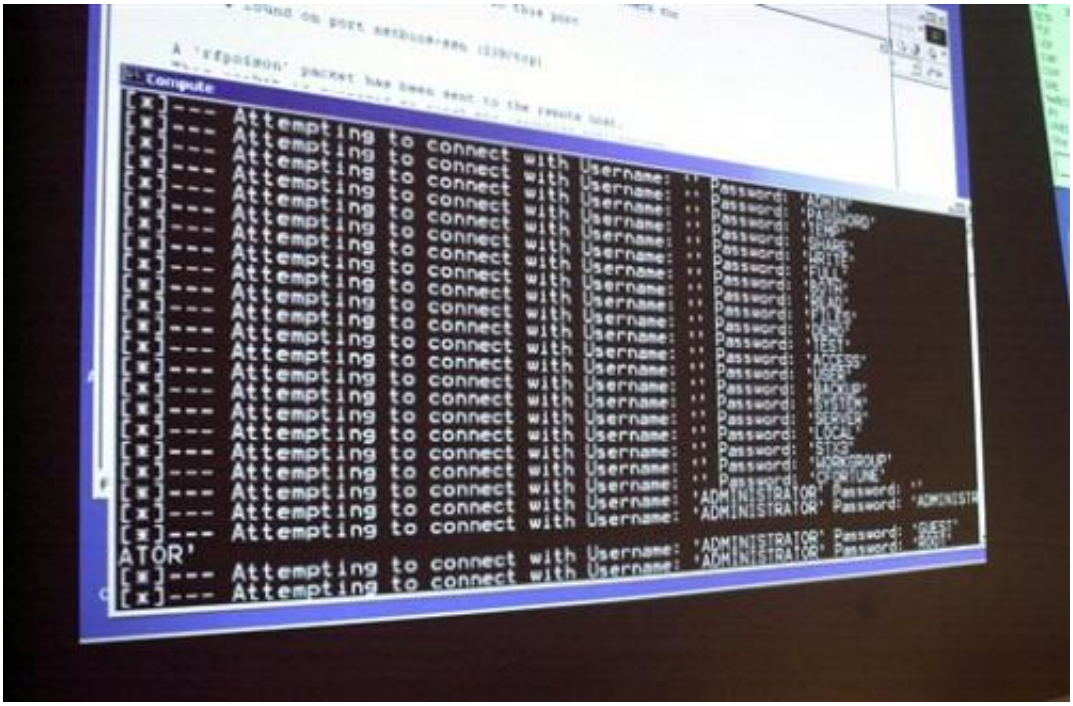
Tech Tips: Guide to protecting Internet accounts

December 5 2013, by Anick Jesdanun



In this Thursday, Jan. 10, 2002, file photo, a computer screen shows a password attack in progress at the Norwich University computer security training program in Northfield, Vt. Security experts said Wednesday, Dec. 4, 2013, that passwords for more than 2 million Facebook, Google and other accounts have been compromised and circulated online, just the latest example of breaches affecting leading Internet services. (AP Photo/Toby Talbot, File)

Security experts say passwords for more than 2 million Facebook, Google and other accounts have been compromised and circulated

online, just the latest example of breaches involving leading Internet companies.

Some services including Twitter have responded by disabling the affected passwords. But there are several things you can do to minimize further threats —even if your account isn't among the 2 million that were compromised.

Here are some tips to help you secure your online accounts:

— ONE THING LEADS TO ANOTHER:

When a malicious hacker gets a password to one account, it's often a stepping stone to a more serious breach, especially because many people use the same passwords on multiple accounts. So if someone breaks into your Facebook account, that person might try the same password on your banking or Amazon account. Suddenly, it's not just about fake messages being posted to your social media accounts. It's about your hard-earned money.

It's particularly bad if the compromised password is for an email account. That's because when you click on a link on a site saying you've forgotten your password, the service will typically send a reset message by email. People who are able to break into your email account, therefore, can use it to create their own passwords for all sorts of accounts. You'll be locked out as they shop and spend, courtesy of you.

If the compromised password is one you use for work, someone can use it to break in to your employer's network, where there are files with trade secrets or customers' credit card numbers.

— BETTER PASSWORDS:

Many breaches occur because passwords are too easy to guess. There's no evidence that guessing was how these 2 million accounts got compromised, but it's still a good reminder to strengthen your passwords. Researchers at security company Trustwave analyzed the passwords compromised and found that only 5 percent were excellent and 17 percent were good. The rest were moderate or worse.

What makes a password strong?

— Make them long. The minimum should be eight characters, but even longer is better.

— Use combinations of letters and numbers, upper and lower case and symbols such as the exclamation mark. Try to vary it as much as you can. "My!PaSsWoRd-32" is far better than "mypassword32."

— Avoid words that are in dictionaries, as there are programs that can crack passwords by going through databases of known words. These programs know about such tricks as adding numbers and symbols, so you'll want to make sure the words you use aren't in the databases. One trick is to think of a sentence and use just the first letter of each word—as in "tqbfjotld" for "the quick brown fox jumps over the lazy dog."

— Avoid easy-to-guess words, even if they aren't in the dictionary. Avoid your name, company name or hometown, for instance. Avoid pets and relatives' names, too. Likewise, avoid things that can be looked up, such as your birthday or ZIP code.

One other thing to consider: Many sites let you reset your password by answering a security question, but these answers —such as your pet or mother's maiden name— are possible to look up. So try to make these answers complex just like passwords, by adding numbers and special

characters and making up responses.

— A SECOND LAYER:

Many services offer a second level of authentication when you're accessing them from a computer or device for the first time. These services will send you a text message to a phone number on file, for instance. The text message contains a code that you need in addition to your password. The idea is that a hacker may have your password, but won't have ready access to your phone.

Facebook, Google, Microsoft and Twitter are among the services offering this dual authentication. It's typically an option, something you have to turn on. Do that. It may be a pain, but it will save you grief later. In most cases, you won't be asked for this second code when you return to a computer you've used before, but be sure to decline that option if you're in a public place such as a library or Internet cafe.

— ONE FINAL THOUGHT:

Change your passwords regularly. It's possible your account information is already circulating. If you have a regular schedule for changing passwords for major accounts, you reduce the amount of time that someone can do harm with that information.

You'll need to decide what counts as a major account. Banking and shopping sites are obvious, as are email and social-networking services. It probably doesn't matter much if someone breaks into the account you use to read newspaper articles (unless it's a subscription).

And strong passwords alone won't completely keep you safe. Make sure your computer is running the latest software, as older versions can have flaws that hackers have been known to exploit. Be careful when clicking

on email attachments, as they may contain malicious software for stealing passwords. Use firewalls and other security programs, many of which are available for free.

© 2013 The Associated Press. All rights reserved.

Citation: Tech Tips: Guide to protecting Internet accounts (2013, December 5) retrieved 13 May 2024 from https://phys.org/news/2013-12-tech-internet-accounts.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.