BIZCOMMUNITY

Do you really WannaCry? A simple guide on how to get hacked

By Melissa Viljoen

14 Jul 2017

If you're like most curious internet users, you've read endless articles about how to protect yourself online. And that's fine if you're a sheep, or you're a chicken, or you want to plaster every surface of your life with bubble wrap...

©rawpixel via 123RF

But for those who seek the exhilaration of living dangerously, here it is at last: the first concise, authoritative guide to making yourself vulnerable online!

1. Click on a link in an email with the subject line verify your bank details

This will immediately infect your computer system with the now-famous WannaCry ransomware virus. You will have the pleasure of seeing a ransom note splashed over your demure desktop, with the demand of a $300 bitcoin payment (in exchange for your now-encrypted data).

You will also have the pleasure of joining government ministries, hospitals, and major corporations in being a part of the worst global ransomware attack in history. Ta daaa!

2. Choose an easy password

For years, the most commonly chosen password in the world was the word, wait for it… “password”.

Of course, that's also the world's most easily guessed password. And there really are professional creeps out there whose job it is to guess passwords and hack their way into accounts.

These lovely characters can actually sell name/password combinations on online hacker forums.

Fortunately, we're making progress. According to SplashData's annual worst passwords list, "password" is no longer the number one most-used password. It's been surpassed by… "123456".

Good work, people.

If you're some kind of risk-averse weakling, it's easy enough to invent a password that's not hard to memorise — but that no hacker can guess (and that no computer program can guess by trying every word in the dictionary, either). For example, you can compose a password from the initials of a fun phrase, like the delicious password "29gofiabm". (That, of course, stands for "29 grammes of fat in a Big Mac.")

So, by all means, save yourself the mental strain of coming up with something hard to guess. Use 123456 or another one of the Top 20 like "qwerty", "iloveyou",
or "abc123".

Global companies attacked, Department of Education hacked, are you armed?
Damian Michael 6 Jul 2017

3. Use the same password for all of your important online accounts

That's right. Use that same, easy-to-memorise password for Yahoo, Facebook, Twitter, Amazon, your bank, and your credit cards. That way, if the bad guys manage to get their hands on one of your accounts, they can also get into all your others. Now you get to live dangerously and you've also made your life a lot easier. Only one password to memorise! #winning

It's possible to have a different password for every site without having to be a national memory champion. You could vary the password for each website — tacking on each site's first initial at the end. For Facebook, "29gofiabmf", for example; for Yahoo, "29gofiabmy".

But you, the thrill seeker, would never bother. Nor would you bother installing a free password-management program like Dashlane or iCloud Keychain (for Apple products). Those programs allow you to have a different, complex password for every site you visit — without you having to memorise anything at all!

But, hey. Where's the thrill in that?

4. Don't surrender your cellphone number as a security measure

These days, websites like Facebook, Gmail, and Yahoo often ask you to provide your cellphone number.

They do that for three security reasons. First, if you forget your password or try to change it, they'll send a new one to your phone for security.

Second, if the company gets hacked or your account gets locked for security reasons, the company has a quick way to alert you — by text message — and let you know the next steps.

Third, some websites, including Google, Facebook, Twitter, and Outlook, offer an optional, super-hyper-secure feature called two-factor authentication. That user-hostile term means this: The first time you log into your account from a new gadget, you have to enter a code that the company sends to you on your cellphone. In other words, hackers using their own computers can never get into your accounts unless they also have your phone.

But you know what? All that's for lily-livered pansies. Want to live on the edge? Keep your cellphone number to yourself!

5. When a bank or another company emails you to report a problem with your account, click the link and log in!

Most of the time, those are fake emails. Clicking the link takes you to a fake website, dressed up to look like your bank's (or eBay's, or PayPal's, or Amazon's or whatever).

When you log in with your name and password, the bad guys intercept it. Now they know your name and password, so they can get into your real websites.

That particular scam — sending a phoney email that seems to be from your bank or another big company — is known as phishing (because they are "fishing" for your information, get it?). And thousands of people every year get scammed that way.

If you think that maybe there really is a problem with your bank, or eBay, or Amazon account, you could open your browser and go log into the company's website the usual way, not by clicking on a link in an email.

If, however, you love the pulse-pounding adrenaline rush that comes from tempting fate, by all means — click on the links in those emails and see what happens!

6. Plug in a flash drive/USB that you randomly found at a café

For all you know, this innocent-looking USB thingy on that cute keyring contains a host of viruses picked up from the seediest places on the interwebs. Of course, it may even be loaded with WannaCry, which would save you from clicking on that shady email link! The pure randomness of the flash drive in your hands – and now in your computer – really says it all…

Now go on, be a daredevil!

Global WannaCry ransomware infection map

18 May 2017

ABOUT THE AUTHOR

Melissa Viljoen is marketing manager, Dial a Nerd.