Veterans For Change™

Est. 2006

Uploaded to the VFC Website

►► ►► July 2014 ◄◄ ◄◄

This Document has been provided to you courtesy of Veterans-For-Change!

Feel free to pass to any veteran who might be able to use this information!

For thousands more files like this and hundreds of links to useful information, and hundreds of “Frequently Asked Questions, please go to:

Veterans-For-Change

If Veterans don’t help Veterans, who will?

Note: VFC is not liable for source information in this document, it is merely provided as a courtesy to our members & subscribers.

How to Get Hacked in 5 Exciting Steps

Most people probably don’t want to get hacked.

Most people don’t want their password stolen by some anonymous Eastern European teenager. They would not like discovering that they can’t get into their own email, Twitter, or Facebook accounts. They would find it embarrassing if their friends all started saying, “Did you know that I’m getting email spam from your account?”

But come on, people. What’s life without a little risk? Doesn’t some danger make everything more exciting? Why do you think so many people still text and drive? Why do you think people still bike without helmets, swim right after eating, and cut off the “DO NOT REMOVE” tags from their mattresses?

That’s right. Because risk makes everything more fun.

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.

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. Choose an easy password. For years, the No. 1 most commonly chosen password in the world was the word “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 get into accounts. They can actually sell name/password combinations in online hacker forums.

Fortunately, we’re making progress. According to SplashData’s annual Worst Passwords List, “password” is no longer the No. 1 most used password. It’s been surpassed — by “123456.” Good work, people.

If you’re some kind of risk-averse wussy, it’s easy enough to invent a password that’s not hard to memorize — 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 grams of fat in a Big Mac.”)

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

2. Use the same password for all your important online accounts. That’s right. Use that same, easy-to-memorize 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 memorize!

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, “29gofiabm**f**,” for example; for Yahoo, “29gofiabm**y**.”

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

But, hey. Where’s the thrill in that?

3. 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 Yahoo Mail, 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!

4. 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 phony email that seems to be from your bank or another big company — is known as *phishing* (because they’re “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 a link in an email.

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

5. When troubles arise, pay for help. No big-name website — Yahoo, Google, Facebook, Twitter, Amazon — ever charges money to give you technical support. (Yahoo, in fact, even has a toll-free help number for “I can’t get into my account” problems: 1-800-318-0612.)

A bunch of bogus “help” sites do charge you, though. They pose as tech-support agencies that can solve problems with your account — for a fee, and often if you agree to give them remote control of your computer.

Only a sucker would fall for such a scheme — or a thrill-seeker like you!

So there you have it: the five easy steps to getting hacked and scammed. Why not make life more interesting for yourself? Start right away!

You’ll be in good company. Hundreds of thousands of people are already following exactly these steps today.