TEN steps to keep from getting your account hacked

The only salvation is in prevention, and this applies to email, social media, and pretty much any password-protected account you might have.

So, what can you do to make sure your account doesn't get hacked into in the first place?

Here are the steps you need to take to prevent losing your account - forever - to a hacker.

Contents

1: Select a good password

You would be shocked at how easy many passwords are to guess. Your pet's name, your pet's name spelled backwards, your favourite TV character's catch phrase, your boyfriend or girlfriend's name (or "ilove" followed by that name), and so on.
If you think people can't guess it, *you are wrong*. They can, and will.

"iLoveMikey" is a *bad* password. "j77AB#qC@^5FT9Da" is a *great* password. You can see the problem though – great passwords are hard to remember.

So, compromise: *never* include full English words or names; *always* include a mix of uppercase and lowercase letters and numbers; *always* make sure that the password is at least 10 or 12 characters long.

"Macintosh" is bad, "Mac7T0sh" might be good, and probably easier to remember. "HondaPrelude" is bad, but "Pre7ood6″ might be ok.

Bottom line: pick a random looking password that YOU can remember, but that THEY would never guess – and assume that THEY are *always really great guessers*.

go to Contents

2: Protect your password

A scenario seen *much* too often starts with "I thought I could trust my boyfriend / girlfriend / husband / wife / co-worker so I shared my password. Then we had an argument."
How much damage can someone do if they're angry with you, and they have the password to your account? A lot.

It's very simple: *Trust no one.* Your friends are your friends until one day they're not. Naturally there are exceptions, but if there's the least little bit of doubt, *don't reveal your password*.
Especially if someone is pressuring you to do so.

go to Contents

3: Set and protect your "secret answer"

Many systems use a "secret question" and its corresponding answer as the key to password recovery or reset. The problem is that many people choose secret answers that nearly anyone can guess. Do people know where you were born? Then they know the answer to that secret question. Do people know what you're pet's name is? Then "favourite pet's name" is probably a bad secret question for you.

And yet people do exactly that. If your account is repeatedly hacked after you recover the password, your "secret question" isn't that secret after all.

A great approach to this is to realize that there's nothing that says your answer actually has to correspond to the question, or to anything else in your life. So, pick an unrelated answer that has nothing to do with you. Perhaps your "City of Birth" should be "Crayola", "Chardonay" or "WindowsExplorer". *As long as you can remember it*, it doesn't matter what it is.

An even better approach is to treat it like just another password - a password to your password, for example. Make it long, and obscure, completely unrelated to the “question”, and impossible for someone else to guess.

go to Contents

4: Set (and maintain!) an alternate email address

Many services will use an “alternate email address” to mail you a password recovery link if you forget yours.
First, make sure to set that option up, and set it up using an email account on a different system. Create and use a Yahoo account for your Hotmail alternate email, for example.

And second: *don’t lose the alternate account*. For many systems, if you can’t access that alternate email account, you cannot get your password back, and you will not be able to recover your primary account.

In too many cases where people lose their alternate email address or let that account lapse, only to be totally out of luck when they find they really need it to recover their primary account.

go to Contents

5: Set (and maintain!) additional security measures offered

Many services now offer additional security measures such as:
Two-factor authentication – requiring that you prove you have your phone by entering a code texted to you, or a number generated by an authenticator app.

Mobile phone account recovery – similar to using an alternate email address, if you ever do lose your password you can authenticate your recovery attempt by responding to or entering a code sent to your phone.

Trusted friends and family – Facebook in particular allow you to designate other Facebook accounts as “trusted contacts” that can be used to validate that you are you and that you should be allowed access to your account.

In almost all cases these measures need to be set up before you need them, so set them up now, while you’re thinking of it. And

remember to change them when, say, your mobile number changes, or your friends change.

go to Contents

6: Use a different password on every site

It's important to use different passwords on each of your important sites.

The reason is very simple: if a hacker manages to discover your password on one account, they very often will go try your username and password, or email and password, on a multitude of other services. If you used the same password on another service that they happen to try, then that account will quickly be hacked as well.

Password safes like LastPass, Roboform and others are excellent ways to maintain multiple, complex passwords for multiple sites without needing to remember each and every one yourself. Speaking of your memory….

go to Contents

7: Remember

Many times, that "hard to guess" is at odds with "easy to remember", but both are absolutely critical.

If you forget your password, and you forget the answer to your secret question or lose access to your alternate email account or somehow lose the ability to use any of the password recovery mechanisms provided by the service … well, to put it bluntly, you are severely out of luck.

Don't forget your own password. Don't forget the answer to your own secret question(s). If you must write your information down *keep it in a secure place*. A sticky note on your monitor under your mouse pad or other, easy to get to place, is not secure. Your wallet might be secure. A locked cabinet or safe might be secure. A properly encrypted file on your computer might be secure.

And once again, a password safe can be used to do the remembering for you.

go to Contents

8: Don't fall for phishing schemes

Phishing is the attempt to represent one's self – typically via email – as someone or some organization that you are not for the purposes of maliciously acquiring sensitive information. *You should never have to email anyone your password, EVER.*

There are some very common phishing attempts that will threaten you with account closure unless you respond to the email with information about your account. Information like your login name and password.

Those emails are bogus. Mark them as spam and ignore them. Any email that requires you to respond with any information that includes your password is almost certainly a phishing scam.

go to Contents

9: Remember that there is little to no support

The vast majority of the account hacks that I hear of – the hacks where people are ultimately unable to recover their accounts – involve free services with little to no support.

There may be a knowledge base, or a peer-to-peer support forum, but there is rarely someone to email and almost never someone to call.

You are responsible for your own account security. It's often true, and certainly safest to assume, that no one will help you should something go wrong.

That means it's up to you to take the preventative measures I've outlined, as well as keeping your information up to date as things change.

go to Contents

10: Learn from your mistakes

Finally, if looking at this list you realize that: the answers to your secret questions are obvious, or you no longer have access to

your alternate email address, or never set one up, or you no longer have access to your old mobile number, or never set one up, or your passwords are short and just plain lame and you use the same one everywhere as well.

go to Contents

Then fix it! NOW! Before it's too late.

If you get hacked and it's for one of those reasons, or you lose access to your hacked account because you never bothered to prepare, you'll kick yourself.

And you may very well lose access to that account forever.