



IT Alley

4742 42nd Ave SW #272
Seattle, WA 98116-4553
www.italleypllc.com
sales@italleypllc.com

How do I safely use a free email account?

Ask Leo! By Leo Notenboom

Summary: Email account theft is rampant. This answer reviews the fairly simple steps and habits you can use to avoid losing your account and the data within it.

My hotmail account was hacked into. I have had this account for almost 9 years, and have never had this happen. I follow a lot of the advice you have given in your article. Now I do remember my password, but do not remember my secret answer. I have spent a great amount of time trying to get help from so called customer service from MSN, but to no avail. As you said it's free, so I guess you get what you pay for. Everyone I know for the most part has been contacted that the email they received is a scam, I don't care about recovering my old email account, just my contacts. Is there any help you can offer.

We have Verizon FIOS, what email do you recommend for the highest protection available today?

Unfortunately you'd have to regain access to your account to get your contacts back (and also hope that the hacker didn't delete them, which they often do).

Obviously, you've been unable to get the account back so I'd consider it a lost cause.

I want to spend a little time with your closing question. I'll phrase it a different way, though, and we'll look at what you need to do so you can most safely use a free email account - or any email account for that matter.

.

It's Not Really About The Service

I'm not going to point at a specific service as having the highest protection. In all honesty, with the problems that I see daily it's not really the service that's causing, or allowing accounts to be compromised, hacked or stolen. In almost every case it's an issue that relates to actions, or oversights by the account owner.

"Put most bluntly, it's usually your fault when your account gets compromised."

Put most bluntly, it's usually your fault when your account gets compromised. Sorry to say it, but that's what I see in my inbox every day.

Yes, some services seem to have a higher rate of compromise, but I relate that more to the popularity of various services as well as the level of technical savvy that comprise the audiences those services attract.

The relative merits of email service providers really comes into play after the account has been stolen. Good providers will help you, the rest will not. While it's not true in absolutely all cases, services which you pay for typically have customer service available to help you, and services which are free do not.

No, avoiding account theft and minimizing the damage when it happens is not up to the provider; it's your responsibility.

Preventing Theft

Preventing account theft really boils down to a list of "don't's" that you've probably heard before. The problem is that some of them are inconvenient ... well, to be blunt again: too bad. Having your account stolen is a lot more inconvenient than any of these steps.

- **Use a good password**; many - perhaps most - account break-ins are from simply guessing your password. Recent studies show that 8 characters is too short. You should consider now need a 12 character password to avoid brute force attacks. Never ever use real words or combinations of words, names, pet's names, or anything that you might find in a dictionary - including a dictionary of slang. Never ever use series of letters like "abcdefgh" or numbers like "12345678". Vary between upper and lower case, and mix letters and digits. **What's a good password?**
- **Don't share your password** with anyone; a common theme I see are accounts stolen by ex-friends and ex-spouses who were given the password back in better days. Planning to change passwords when you break up doesn't work - often the account theft happens *before* the breakup - or even causes it.
- **Don't write your password down** - at least not in an easily accessible place. If you must, then keep that in a locked drawer for which only you have a key, a safety deposit box or something similar. *Written down passwords will be found.* Consider using an encrypting password storage system like LastPass or **Roboform** to remember your passwords.
- **Don't login to your account on any computer you don't control** - ever. Public computers are a gold mine for people that want to steal accounts. Intentional or otherwise, you have no idea what's on that machine - be it a key logger, or some way of recovering the password after you've logged in. I regularly hear from people who logged in to check their email at a "friends" house, or worse - a public library - and their account is quickly and easily

stolen. **How can I be sure my actions aren't being logged on this computer I'm using?**

- **Don't login to your account over an unencrypted open WiFi hotspot connection.** Anyone within range could be watching your login information as you send it and can capture your user name and password. Encryption is safe, but not all services use it, or use it properly. If you're not sure it's properly encrypted, don't login. **How do I stay safe in an internet cafe?**
- **Keep your machine clear of malware.** This could be another list of "don't's" all by itself. Don't open attachments you don't expect, don't download from sites that aren't known to be absolutely trustworthy, don't accept unexpected file transfers, and so on. Run up-to-date anti-malware software, and get behind a firewall of some sort. **Internet Safety: How do I keep my computer safe on the internet?**
- **Don't fall for phishing scams.** No legitimate service will ever ask you for your password over email. This form of account theft is on the rise as people are responding to bogus threats that their account will be closed. If you're not sure, check with your provider directly by visiting their web site. Do not respond to email that asks for your password - *ever*. **Phishing? What's Phishing?**

Almost all of those recommendations apply regardless of what email service you use, and regardless of how you access it. In fact, those recommendations apply to any online service, not just email.

And if your account has been compromised, I'm willing to bet that 99 times out of 100, one or more of those recommendations was not being followed and lead to the theft.

Recovering From Theft

If you plan ahead you can make recovering from account theft a little less painful, and a lot less catastrophic in terms of lost data.

- **Use a paid service if you can.** I've been saying this for a long time, and my reasoning is very, very simple: free services have limited or no customer support - paid services typically have real live people to help you in a crisis. Not all are created equal, so do some research, but as a general rule of thumb what you're looking for is someone to help you recover your account should it ever be compromised. To me that means a customer service desk that's accessible and helpful. **What for-pay email providers do you recommend?**
- **Use a desktop email program** like Outlook, Thunderbird or any of a hundred others. Even the free services like Hotmail or Gmail will let you do this now. What this does is place your data on your machine and in your control. If you lose access to the account for some reason your address book,

your email, your whatever-was-in-there is still on your machine. You'll have lost none of it. Yes, this does require that you take responsibility for your machine, your mail and backing up your data - but you should be doing that already anyway. **What are the pros and cons of web-based email over desktop email?**

- **If you can't use a desktop email program, then backup your data -** regularly and often. Periodically export your address book and save it on your PC (where it's regularly backed up, right?). Download your email every so often with a desktop email program, or perhaps auto-forward all your email to another email account. CC yourself on every sent mail so you have that too (most auto-forwards do not affect sent mail, and most desktop email programs download only your inbox).
- **Remember your secret answers.** It amazes me somewhat how often people forget these. You want them for two reasons: they're required for automated recovery of you password should you forget or lose that, and knowing these answers is one way that customer service people can be sure you really are the proper account owner. If you don't know they can't trust you - anyone could contact them and say "yes, it's really my account, honest!" - it's those secret answers that prove to them that you are the rightful owner.

It Only Seems Daunting

That's a loooooong list of do's and don't's, but don't let it discourage you. Many are simple and common sense habits that once developed will help you keep your account information, be it email or something else entirely, safe.

While I hear every day of people who've lost their accounts without hope of recovery, remember - there are many, many more I *don't* hear from. These are the folks who've taken responsibility for their account security and made these recommendations second nature. It's just how they use their computer.

Safely.

And without ever having had an account hacked, or data lost because of it.