Steps To Take If Your Information Is Found On The Dark Web

A lot of people don't know what to do when their email is found on the dark web.
Is it a code-red emergency? Or just a small nuisance? Well, we're going to give you everyone's favorite answer…

It depends.

Sometimes having your email found on the dark web means you have a major problem on your hands, and sometimes it just means you have to change a couple of passwords.

But here's the thing:

Not knowing the level of severity when it happens means you need to take it seriously regardless.

The problem is most people don't know where to begin. They start randomly changing passwords, deleting accounts and calling their bank without rhyme or reason.
They know they should be doing something, they just aren't sure what.
That's why we've put together this quick checklist you can use if your email is found on the dark web. It keeps things simple and will make sure your personal information stays away from prying eyes.

Should You Panic If Your Email Is Found On The Dark Web?

This is the first thing that most people wonder when their email is found on the dark web. How worried should you be about this?

Like we touched on before, it depends on the situation. But let's take a second to explore the possibilities (and illustrate why you should take care of this ASAP).
If your email is found on the dark web there's a chance that it's nothing more than that, an email address that the public can see. It doesn't mean anyone has hacked into any of your accounts, or accessed any other information.

However, there's also another possibility.

Having one of your emails on the dark web can kick off a chain reaction that no one wants. Hackers and scammers regularly check the dark web for accounts they can use for their nasty practices.

There are a number of methods that can be used, but the most important thing to focus on is the fact that they'll try anything.

This means if your email is found on the dark web the likelihood that you'll become the victim of a phishing scam goes through the roof. It also means there's a chance someone else will gain access to some of your accounts. It might just be an old profile, but it could be your Amazon account (yikes). This is why we say that you need to take the situation seriously if this has happened to you. Just because the sky hasn't fallen, it doesn't mean something awful might not be happy in the near future.

What should you do?   This will depend on the types of personal information involved.

Financial and other account numbers. Notify the places where you have those accounts. You may need new account numbers and to make other changes to stop those accounts from being misused from that point on. If fraud has already occurred, ask what you need to do to clear up the problems. You have the right to challenge credit card charges and debits you did not make.

Passwords. Change them. And if you've used the same passwords for multiple accounts (a common but dangerous practice, since crooks often try them in several different places to see if they work), be sure to change them everywhere.

Driver's licenses and passports. Contact the agencies that issued them.

Email address and phone number. It's probably not worth the hassle to change them, but be on guard for your email address being used to send spam or your phone number being "spoofed" to make calls look like they're coming from you. Contact your service provider if that happens.

Social Security number. This is the most dangerous type of personal information in the hands of identity thieves because it can open the gate to serious fraud, from obtaining credit in your name to impersonating you to get medical services, government benefits, your tax refunds, employment – even using your identity in bankruptcy and other legal matters. It's hard to change your Social Security number and it's not a good idea because it is connected to your life in so many ways. There are a number of things you can do, including alerting the Social

Security Administration, Internal Revenue Service and by placing fraud alerts on your credit files.

Medical records, diplomas and other personal information may also be found for sale on the dark web. At the Federal Trade Commission's www.identitytheft.gov website you can get step-by-step instructions for what to do, tailored to your specific situation. The nonprofit Identity Theft Resource Center also provides free help for identity theft victims. Go to www.idtheftcenter.org or call 888-400-5530.

If you are a data breach victim, take advantage of free identity theft services if they're offered. Thinking about buying identity theft services? Shop around and make sure you understand how they work, what they cost, and what help they provide if you become a victim before deciding whether to sign up and which one to choose. Do not be swayed by scare tactics, claims that an identity theft service can prevent you from becoming a victim, or million dollar guarantees.

Additionally, here are some steps to consider:

1. Scan Your Computer

We believe that starting with a virus scan of your computer is the smartest thing to do when your email is found on the dark web. Doing this before changing any passwords is the safest possible course of action.

Why?

There is a long list of viruses that can all monitor your activity and log your keystrokes and passwords. This sort of thing has been around for a while. If you happen to have one of these forms of malware on your computer, changing all your passwords will be a waste of time. Those will all get logged as well. This is why it's crucial that you do a double-check of the security on the computers you use to log in to various accounts. Even if you're someone who stays on top of this sort of thing, all it takes is one virus to slip through the cracks.

You probably have some sort of antivirus software pre-installed on your computer already, so start with them. If you don't, there are plenty of free options to get you started. Kaspersky for PC and Avast for Mac are two great options.

Once you're sure that you don't have any malware on your computer that's responsible for your email being found on the dark web, you can continue on to the next step.

2. Step Up Your Password Game

This is the most common fix people think about when they find their email on the dark web. There's a reason for this, it works.

Emails found on the dark web are far more likely to be the victim of phishing scams and hacks. These are far more likely to be successful when passwords haven't been changed, or if the same password is used for all accounts.

Quick tip – If you want to create a password that's as secure as possible it should have the following traits:

- Be lengthy. 12-15 characters is a good target
- Avoid using real words
- Combine uppercase and lowercase letters
- Add numbers and symbols

First, you should deal with the email in question. You'll want to change the password you use to access it and consider setting up two-factor authentication (more on that later). This is often the first place attacks start when an email is found on the dark web, so it makes sense to protect it first.

Then you'll want to work your way down the line of any websites or accounts tied to this email address. Each of these will require a new password too.
If you want to play things super safe you can create a separate password for each profile you have. This will require you to use a password manager like 1Password or LastPass (unless you have a freakishly good memory).

If you'd rather not go that route, we recommend coming up with two or three passwords that you can remember on your own and spread those across your various accounts and profiles. Then replace them every few months.

3. Make A Garbage Email

During this stage, you might want to consider creating another email account that can be used for unimportant profiles. So many sites require a sign-up process these days, and having them tied to your main email account isn't ideal.

The reason for this is if there's a data breach on one of these unimportant websites, your primary email won't be found on the dark web. It's way better to have a burner email floating around than the account you use for banking and other important tasks.
Another advantage of this is it will save you time in the long run. If this garbage account is truly tied to websites and profiles you don't care much about, you can always just

scrap it and move on. You won’t need to spend a ton of time going through each site and updating all passwords.

It might seem like a pain to have multiple email accounts, but it’s really not that much extra effort. It only takes a minute to create a new one, and the additional security it provides makes the time spent a no-brainer.

Some people even run with three email accounts to protect their most important information even further.

This will typically look like one primary account for business and banking, another for personal correspondence and important accounts (like Amazon or Facebook), and a junk account as a catch-all for what’s left.

This means that your most important accounts are further protected from a breach and if one of these emails is found on the dark web, there’s less damage control you’ll have to do afterwards.

4. Check On Your Financial Accounts

A Brief Panic Squelcher: This is rarely an issue for people with emails found on the dark web, but it’s smart to go through this process anyway.

At this point, you should’ve already updated the passwords tied to any banking websites you use (and ideally set up two-factor authentication).

Now it’s time to take a closer look at your accounts.

Make sure no money is missing and no strange activity appears to have occurred. If you notice something, get in touch with your bank.

If everything looks fine, check back in a week or two and verify. Then do the same thing a week or two after that. Sometimes hackers will wait a while before they try to sneak in a purchase or two.

If you want to check on your financial accounts but don’t feel comfortable using your computer yet (maybe you found a virus that hasn’t been cleared out yet), you’ll want to be careful accessing your account.

Assuming you have a smartphone with a data plan you can use that to access your accounts with little risk. Disconnect your phone from your wifi network and use your data plan to access your accounts. Doing this won’t use much data and will prevent you from potentially using a compromised wifi connection.

5. Practice Smart Transaction Habits Going Forward

You should be doing this in general, but having your email found on the dark web means it’s time to be extra diligent.

Only make purchases on websites that are trustworthy and reliable. While there’s no foolproof site or company to buy from online, doing this will help reduce risk significantly.

Websites that don’t have “HTTPS” at the beginning of their URL should be ignored immediately (you can check this by looking at the address bar in your browser). It doesn’t if they have the coolest jeans in the world on their site, it’s simply not safe.
If you do this you’ll be far more likely to have your information protected when you make purchases online, and the chance of your email showing up on the dark web will decrease significantly.

6. Try Two-Factor Authentication

If your email has been found on the dark web it’s probably a smart idea for you to use two-factor authentication for your most important accounts. Two-factor authentication adds an extra layer of security and makes it significantly harder for a hacker to gain access.

Here’s how it works:

Usually, you enter your email address and password to log in to an account online.

That’s all it takes.

With two-factor authentication, you add one very important step to the process. After you submit your standard information you’ll need to verify the login attempt. This is typically done by receiving a text message with a random code you’ll need to enter to access your account.

This prevents a third party from gaining access to your accounts, even if they have your email and password.

You’d be surprised how many websites can be tricked into giving out access to your account to someone even if they only have your email address. This is why it’s important to do all of the recommended steps if your email is found on the dark web.

7. Opt Out From Data Brokers And People Search Sites

This is one method that gets overlooked far too often, and it’s a huge shame. Because this is probably one of the most common reasons why people end up finding their emails on the dark web.

Data brokers and people search sites like Whitepages and FastPeopleSearch exist solely for the purpose of sharing your info (like your email). These sites then get scraped by spammers and hackers to build massive databases of info they can abuse.

This means you need to get your info off of them ASAP.

You can do this by manually opting out of each site (which will take a little time) or by doing it automatically. These sites legally have to honor your request for removal, so it's only a matter of submitting them. No matter which method you go with, you should get started as quickly as you can. The sooner your sensitive information is off the web for anyone to look up, the sooner you can relax.

What's Next?

If you've followed the steps above, then you're in pretty good shape right now. You're way more secure than you were before, and the chance of another email being found on the dark web is much lower as well.

But here's what you have to remember:

All it takes for you to end up in this mess again is getting lazy with your passwords or purchase from an unsecured site. You could be doing everything 95% correct, and still end up with another email on the dark web for everyone to see. So take your use of the internet seriously.

As much as it would be great to not have to worry about hackers and spammers, they aren't going anywhere. So make these steps and habits second nature when you're online.

If you do, you'll be alright.