REPUTATIONDEFENDER®

The Ultimate Guide to Protecting Yourself Online

Online security is a bit like the newest household chore. We know it's important and we do our best to keep up with it, but somehow few of us are as thorough as we'd like to be.

Anyone who reads this blog regularly already knows they should change passwords often, use a unique, individual password for each site, and check frequently to see if vulnerable personal data is available online. Still, how do people have time to make this part of a daily or weekly routine? Looking at the number of celebrity hacks and internet missteps, it's clear that even the most successful people don't fare much better.

This Reputation Defender guide will help lay out the most important things you can do to protect yourself online. This is doubly important for high profile individuals who represent a much bigger target for hackers. Reputation damage can be a problem in almost any career and keeping security and privacy settings up-to-date will go a long way to prevent the issue.

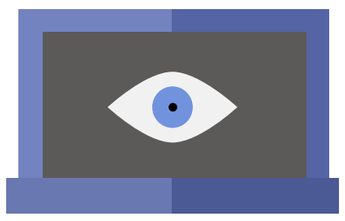
Step-by-step guide to becoming worry-free

The following measures may take up to an hour depending on how tech savvy you are. Not long to spend to keep you and your family safe.

You may want to break the work down to focus on security in one session and privacy the next. Once these steps are complete, you'll be able to get on with your life, free from any immediate concerns over internet vulnerabilities. If you are someone who spends a lot of time forgetting their password, you will probably stop needing to request password reminders.

Online Security

- **Choose a password manager**
- **Update your accounts**
- **Create a master-password**
- **Two-step verification**



Online Privacy

- **Check your address**
- **Check social media settings**
- **Verify other family members**

REPUTATIONDEFENDER®

Online Security

Did you know?
86% of internet users have taken steps online to remove or mask their digital footprint

Step 1: Choose a password manager

This is the first step in any online security makeover. It's not as simple as it might sound given the range of password managers available, from free versions to those with a yearly fee or a one-time license cost.

LastPass is the easiest and most popular option. It comes as a free download, but to include your mobile phone you will need the premium version. LastPass had some security issues in 2015, but most people agree it was well handled. According to security expert Troy Hunt, "their hashing approach was solid and designed to be resilient." LastPass is a cloud based system so your passwords will be stored in the cloud, however they will be downloaded to your computer before they are un-encrypted.

Other systems like **KeePass** and **1Password** opt for offline storage which is slightly more secure. Passwords can still be manually synced between devices, but they are stored on your computer or on a USB drive rather than the cloud. **Dashlane** is another well-rated option that is secure as well as easy to use, but the more expensive yearly fee can be prohibitive.

Step 2: Update your accounts

Once you've chosen and downloaded your password manager, you will need to go through all your accounts to store each password in your password manager.

Make a list of every account you can think of, from bank accounts to social media pages, to Amazon.co.uk and other places you order online, and go through them one by one. Unless you already have a strong password system, you will want to let the manager generate a new, unique password for each site. If you prefer to keep your existing passwords, some models like **LastPass** will capture these and highlight weaknesses, however it's generally easier to let the manager generate and remember passwords.

Continue!

REPUTATIONDEFENDER®

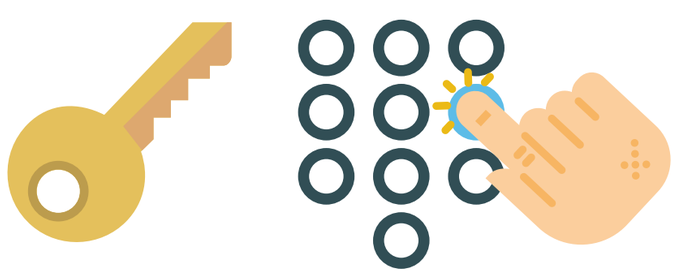
Online Security

Did you know?
21% of internet users have had an email or social networking account compromised or taken over by someone else without permission

Step 3: Create a master password

You will need to choose a **secure, memorable master-password** for the manager itself. Try using the first letters of a unique phrase and substitute capitals, numbers, and symbols for some letters.

Avoid giving yourself hints that could make your master-password too easy to guess. Remember, this password will allow access to all your accounts, so it needs to be memorable for you but un-guessable to anyone else.



Step 4: Add two-step verification

Many sites like **Twitter, Facebook and Gmail** now offer **two-step verification**. It's important to activate this measure since it will protect you in case of a security issue with your password manager.

Two-step verification will send a code to your mobile phone or another email address which you will then be required to enter in order to sign on. This measure will kick in anytime you change your password or sign in from a new computer. If you think this sounds cumbersome, remember how many emails and texts you receive on a daily basis. You'll rarely be trying to access your account without your mobile phone immediately handy.

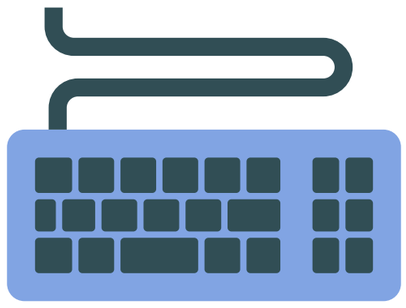
There are no fail-safe measures when it comes to the internet security, but the steps listed above will make your accounts much harder to hack.

Continue to Online Privacy

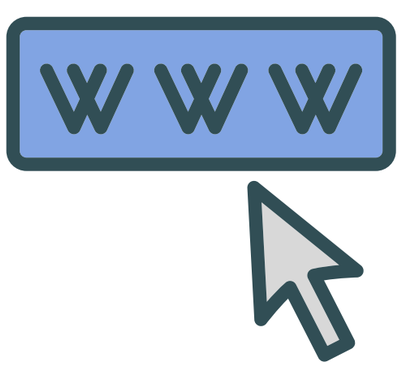
REPUTATIONDEFENDER®

Online Privacy

Did you know?
6% of internet users have been the victim of an online scam and lost money



Next you will need to update your internet privacy to limit public sharing of details about your location and personal life. This can be a security risk also, since access to personal data will help hackers get past the security measures you just put in place.



Step 1: Check your address

Professionals who own their domain name may find that their location and personal details are available online on **Whoisnet**.

If this is the case, contact the service where you bought your domain name, and update your privacy settings, so your data won't be visible online. Other vulnerabilities in the UK include **Freelectoralrolls.com** and **Companies House** which may list your address online. You can contact your local electoral registration office and ask to be removed from the public records.

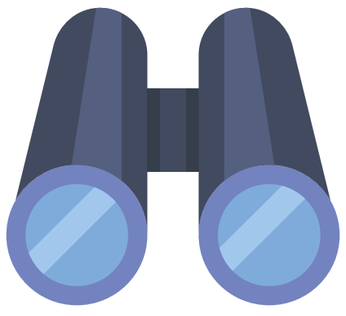
If your personal address is available through Companies House contact them directly also, and ask that anything unrelated to your professional profile be removed. To avoid being identified you will need to contact each one and ask to have your personal data removed.

Continue!

REPUTATIONDEFENDER®

Online Privacy

Did you know?
12% of internet users have been stalked or harassed online



Step 2: Check your privacy settings

If you have social media accounts, even if you rarely use them anymore, they can be a big potential information leak. **Double-check your settings** to make sure you're not automatically sharing pictures or posts publically and that old albums and posts are private.

If you have a lot of social media accounts, you will need to make a list and go through them all one by one to make sure you don't miss any. Remember, if you click share on an article page, this will always be public. It's much better to copy and paste the address into your post.

Step 3: Verify family members

It doesn't matter how careful you are about security and privacy, if family members don't take the same measures your efforts can fruitless. This is even more important for companies based on a family name since everything relatives do online will reflect back on the brand.

Admittedly pushing your family to run through all the same measures listed in this article might not be easy. Once you've learned the ropes, try sitting down together and making a fun interactive security day.

More security options

Other Security Options

Did you know?
50% say they are worried about the amount of personal information about them that is online

You've completed the basic security and privacy measures listed in this ultimate guide, but you're still concerned about what happens if your computer or mobile phone is hacked. If this is the case you can keep going with your makeover by installing programs that will protect you in the event of an identity or data breach.

Little Snitch and **Wireshark** are two options that will show exactly what data your computer is sharing. These programs warn you immediately if your computer is hacked so you can take action right away. Another important protection for your mobile phone is **Prey**, a program that lets you wipe data in the advent that your phone is ever stolen.

None of these measures are absolutely necessary if you've already updated and double-checked your settings as outlined in the guide, but they do add an extra layer of protection. If you need more information or advice on specific online threats, our privacy experts at **ReputationDefender** are always ready to help.