GOLDBERG & OSBORNE
The Injury Lawyers & Consumer Advocates
1-800-THE-EAGLE
www.1800theeagle.com

Guide to Protecting Your Identity, Privacy, and Reputation Online

These days, many people live their lives online. They post pictures of what they ate for breakfast, network on LinkedIn, tweet about politics or their favorite band, do their banking, pay their bills, and shop for everything from a toothbrush to a house.

Online life is now such a normal part of everyday living that many people fail to recognize the potential dangers. Or, maybe they recognize them but are uninformed about the security measures they can take to protect themselves.

Without adequate security, your identity, privacy, and reputation are at risk. Even if you delete the post, it lives on, forever. Read on to discover how to protect yourself online.

How to Protect Your Identity Online

Identity thieves search for any personal information they can find about you. This includes your name, birth date, family connections, social security number, and driver's license number. Most people learned about shredding sensitive documents years ago, but may have missed the lesson about how easy it is to glean this information from your online presence.

If you aren't careful, your social media profiles offer a wealth of information about you, such as email address and birthday. If you're friends with your mom online, they likely know your mother's maiden name (that doesn't mean that you shouldn't be friends with your mom online).

Online security goes beyond setting your online status to Private, though. It starts with locking the door.

How to Strengthen Your Passwords

If a password is easy for you to remember, it's probably a bad password. Names of family members or pets, dates, pretty much anything that's an actual word is vulnerable to hackers.

A strong password is the first step toward protecting your identity online, and it must meet two basic criteria:

- Be at least 10 characters long
- Contain both upper- and lowercase letters, as well as numbers and special characters

What's more, you need different passwords for every site, and you need to change them occasionally. Now you're wondering how in the world you'll remember multiple passwords of nonsensical gibberish. That’s why you need a password phrase.

The password phrase allows you to create a wholly unique password that fits all the criteria, yet is easy for you to remember. It can be a line from a song or your favorite book, a quote, or anything you want it to be, so long as it's memorable to you.

Example: The only thing we have to fear is fear itself. Now, choose a letter, number, and special character for each word in the sentence, such as T0twH2F!f!. You can customize it for each site while keeping the core password the same. For example, add a P at the beginning and end for your PayPal account, or an E and M for your email account.

Once you land on your personal substitution code, memorizing it is simple, and it's a lot more secure than Fido929.

Steer Clear of Public Wi-Fi

Whether you're working at the coffee shop or streaming Netflix during your break at work, free Wi-Fi keeps you from blowing your monthly data allowance.

It comes with a different price though, and that's lack of security. Wi-Fi hotspots are extremely vulnerable to hackers, and there are many of free apps and programs that allow users to capture every keystroke on a network. That means that every site you visit and every button you click is potentially visible to the hacker.

If you rely on free Wi-Fi and want to protect yourself online, you should consider using a VPN (virtual private network). There are many of them out there, and they keep you anonymous while you're online. A VPN connection will add a level of security to your internet browsing by encrypting your internet connection and allowing you to surf the net privately. Hackers will not be able to interpret what you are doing. Consumers can purchase a VPN service rather easily for about $5 to $10 per month. You can obtain more information on websites such as www.privateinternetaccess.com. You can also search online “How to obtain a VPN” to get results that will lead you to helpful information.

Basic Identity Security Steps

Setting up secure passwords and anonymous browsing are important, but they aren't the only steps you can take to secure your identity online. Additional methods of protection include:

- Turn off location/GPS and Bluetooth when you aren't using them.
- Add a strong password to your home Wi-Fi to protect it from hackers.
- Monitor your bank statements for suspicious activity.
- Never click links to financial sites from an email; always log into the site through your browser.
- Never complete financial transactions on an unsecure site; you know it's secure if the address reads "https" instead of "http," and it displays the lock icon.

How to Protect Your Privacy Online

You now have strong passwords, private social media accounts, and a clean Internet connection. Your next step is guarding your online privacy, which has the added benefit of protecting your identity.

Let's look at your social media profiles again. Just because you *can* enter a boatload of private information does not mean that you *should*. Your real friends already have your email address and phone number, and they probably know your birthday. There's no need to enter that information, though hackers hope you will.

You should also set your browser to private, available in the advanced settings of all the major browsers. This deletes cookies and clears your browsing history, and keeps ad networks from tracking your every move.

Finally, establish multiple email accounts to guard your privacy. They're free, and it's a simple way to protect your private email from spam and hackers, as well as protecting your sanity from endless promotional offers.

Three email accounts should handle your needs. The first is your "real" email address for communicating with actual people whom you actually know. The second is for your social media accounts. The third is for things like loyalty clubs, online shopping, newsletters, and similar communications. For those who have gmail accounts, or are interested in opening a gmail account for your email needs, visit http://fieldguide.gizmodo.com/how-to-use-the-infinite-number-of-email-addresses-gmail-1609458192 to learn how to utilize your email account for this purpose.

It may feel like a hassle to take these steps. Only you know if your privacy is worth the time it takes to ensure it.

How to Protect Your Reputation Online

The Internet did much to make our lives easier, but it comes with a couple of downsides. One of these is how easy it is to destroy someone's reputation.

Remember, once you post something online, you lose all control of it. Photos, quotes, stories, tweets; anything has the potential to wreak havoc on your life. Once it's out there, it no longer belongs to you. Flooding the internet with positive stories is your only hope of burying the story.

However, this is easier said than done. Search engines rate content in a number of ways and one of these is by how often a piece is viewed. It's far simpler to exercise caution to reduce your risk. What does this look like?

- Think before you post. Would you be ashamed to show your children or grandparents what you're about to post? How would you feel if your boss saw it?
- The photos from your bachelor or bachelorette party may document a fun night, but you really don't want them on the Internet. Laugh in private, but don't hit Post.
- Don't send personal or inappropriate emails from your work account. Those things have a way of coming back to haunt you, and you never know when it will happen.
- Separate your personal and professional sites. Maybe Facebook is for family, Twitter is for your political rants, and LinkedIn is the only place where you connect with professionals. Remember, you don't have to accept every friendship request.
- If you already have a mixture of friends, family, and colleagues in Facebook, create groups to manage who sees what.

It always goes back to the top item: think before you post.

Be Proactive

Of course, this advice doesn't protect you against malicious attacks, such as cyberbullying or negative attacks against your brand if you're an entrepreneur.

If you aren't familiar with the term, "cyberbullying" is a type of online harassment designed to destroy the victim's reputation. It happens to kids and adults, and does a lot of damage. Let's face it; the anonymous nature of the Internet brings out the worst in a lot of people.

Cyber attacks can be hard to combat, but you can mitigate them by establishing a strong, healthy online presence *before* there's a problem. In other words, if you have a lot of positive content online before a cyber attack occurs, you have an easier time bouncing back from it.

The easiest option is to start a blog and post consistently (weekly, not daily). You can center it around your professional area of expertise, a hobby, or review your favorite books and movies.

Like your social media presence, keep it clean and professional (especially since the goal is protecting you against potential future cyber attacks). It takes time to build up an online presence, at least six months and 12 is more realistic, but it serves two purposes. First, it gets your name out there and helps you become known. Second, of course, is to build your reputation high enough that knocking it down won't be easy.

Disposing of Old Computer Equipment

To properly dispose of old computer equipment and clear it of any private history, it is recommended that you take your device or computer to a recycling facility or retail location that specializes in helping people with their computers. If you plan to sell the device, at the very minimum you should perform a factory reset.

For instructions on how to do this, search online for “How to factory reset XYZ” (XYZ being the device make and model). Note that factory resetting doesn’t guarantee complete sanitization. Data on hard drives may still be able to be read by knowledgeable individuals even after formatting and/or a factory reset as the data has not been truly overwritten. If the device contained sensitive information such as bank accounts, passwords, etc., it is recommended that you seek the help of an expert to securely erase the hard drive. If you would like to try this yourself, you can use software such as Eraser for PC or visit https://support.apple.com/kb/PH22241 for Mac instructions.

Security Takes Time

The real takeaway from all of these steps is that it takes time and effort to protect yourself online. If you value your privacy and reputation, and hope to protect your identity, these efforts are well worth the time.

Disclaimer: This guide is provided only for informational purposes and is not intended to be a substitute for legal or other professional advice. This guide does not contain nor is it intended to provide legal or other professional advice for any specific situation and readers should not take action or refrain from taking action, based only on the information provided in this guide. Goldberg & Osborne has attempted to provide accurate and current information in this guide, but cannot and does not guarantee that the information is accurate, complete, or up to date. This guide may contain links and/or search terms that will lead to external websites as a convenience to the reader, but Goldberg & Osborne is not responsible for the content or operation of any website other than its own website. The presence of a link or a search term does not imply and is not an endorsement by Goldberg & Osborne of the website provider or the information contained on any linked website or on any website contained in search results from a search term provided in the guide.