Safeguard Your Online Information

Practical Ways to Keep Your Data from Falling Into the Wrong Hands

With so much of our business happening online these days, it's no surprise that hackers put a great deal of effort into trying to access your information. According to data security firm Positive Technologies, billions of people had their information breached in 2018 alone – including 500 million when Marriott Hotels was attacked in September.

What can you do to protect yourself? Here are a few real-world strategies to keep in mind:

Be Mindful of What You Share

There are certain pieces of personal information you should never share on anything but the most secure sites, such as account numbers and passwords. If you're entering these things on a website, make sure that site belongs to a trusted entity and double-check to make sure it's the legitimate, secure site rather than a lookalike created by hackers to capture your information. Some things to check include looking in your browser bar to verify the site is secure and searching for the company in another tab so you can compare web addresses.

If you get an email asking for personal information, don't click links in the email. Type the company's name into your browser and verify the request before entering any information. Also, no reputable company would ask you to type sensitive information into a reply email. A good policy to follow: Only provide sensitive personal or financial information during a transaction you've initiated yourself.

It's sometimes difficult to conduct business online without giving out your Social Security number, but remember that is the lynchpin to your entire identity in the modern world. The decision to share it is always yours and you can always choose not to do business with a site that needs your SSN. If you're at all uncomfortable with such a request, ask what happens if you don't provide the number and how it will be protected if you do.

Be Creative with Your Passwords

The problem with most modern password strategies is that anything strong enough to secure your information can be difficult for you to remember. English words are easier to hack, but proper names can be easier for you to recall and harder for hackers to guess. With so many sites requiring special characters for passwords now, simple

character substitution, like ! for I or $ for s can make what might otherwise be crackable passwords into easy-to-remember ciphers: “Bre++F@vre4,” for instance.

Another helpful strategy is to use a password manager, like LastPass or Dashlane. These apps store your passwords in a secure, offline place, then enter them every time you need to login to a site. These are often available for free, although the strongest security often comes with more expensive packages.

Something to keep in mind if you reuse your password across multiple sites: If any one of your accounts gets breached, that password may now be in the hands of hackers. If you use the same login credentials on other accounts, the criminals may have access to your other accounts as well. If it’s too much to use a unique password for each of your online accounts, you should absolutely change all of them if any one of your accounts is breached.

Limit Social Sharing

It’s important to know who can see what you share on social media. While no one is going to post their bank account number in such a public forum, linking to people you don’t know can offer them insights into things like when you’re away on vacation.

Platforms like Facebook have a privacy setting that can limit who sees what you post, but the best way to control access to details about your life is to be discerning about what you choose to share, where and why.

Also try to make sure you know the people you friend or add via social media in real life. If someone’s behavior – particularly someone you don’t know well – seems suspicious, don’t hesitate to block or delete them.

Safely Dispose of Old Information

By now you’ve probably opened dozens of online accounts, many of which you never use anymore. But if there’s a breach at one of those forgotten entities, hackers may have access to whatever personal information is tied to that account. An old email account, for instance, could be holding past bank statements filled with personal data that could lead to identity theft.

One rainy Saturday afternoon, take some time to try to track down all the online accounts you don’t use anymore, and shut them down to the best of your ability. Delete old messages, statements or emails and change the passwords. The less personal information you leave in these orphaned accounts, the better.

Similarly, before you dispose of a computer, use a wipe utility program to overwrite the entire hard drive. For a smartphone, you'll want to remove the memory card or SIM card. To the extent that you can, delete your contacts, messages and voicemails as well.

In the modern online world, information never really dies. The best you can do is try to keep it out of the hands of those who could use it to harm you.