YOUR ESSENTIAL GUIDE TO ONLINE SAFETY

Consumer Reports, Feb. 2021

Part 1

- **It is extremely difficult to remove your information from the web**
- **It is a continuing exercise to keep it off**

Examples of the difficulties in removing your data:

1. The data brokers claim they need all kinds of small personal details to confirm an individual's identity before removing their data. For the suppression to be accurate, it is requested that the individual provide all variations of their full name. That might include nicknames, former names, married name, common spellings, or misspellings.

2. People who track the problem estimate that it can take from six business days to two weeks of fulltime work to delete your information from data brokers' sites.

3. The companies were continually trawling driver's license registration records, voter registration databases, and address information from the U.S. Postal Service, creating new listings to replace the ones I had removed.

Part 2: Scrubbing Your Info From People Searching Sites

REMOVING YOUR DATA from peoplesearch sites isn't a one-time task: After you take the following steps, you'll have to check to make sure your info is gone, then repeat the process as it reappears, **around twice a year**

Because it's time consuming, you may want start with a few of the best-known sites, such as BeenVerified, PeopleFinders, Pipl, Spokeo, Whitepages, and ZoomInfo. (I maintain a list of more than 50 sites' opt-out links; search online for "Big Ass Data Broker Opt-Out List.")

First, check each site to learn whether it has your information listed. Then see what each data broker requires for you to opt out. Some make you send a letter or fax, or call by phone. Others ask for personal information before they will scrub your data, so be cautious.

You can pay a service to do the opting out for you.

While none promise to remove your data from every people-search site out there, here's what leading companies currently offer:

DeleteMe removes your info from 41 sites every three months ($129 per year, or $229 for two people).

PrivacyDuck will do a monthly data removal for two people from 92 sites ($499 per year) or 191 sites ($999).

OneRep deletes info from 96 sites ($100 per year per person, or $180 for a family), with a pricier option for the most challenging sites.

Part 3: Your Digital Security Action Plan

1. Get a Password Manager (CR recommends 1Password, Keeper and BitWarden

2. Use Multifactor Authentication (MFA) also known as two-factor authentication (2FA) whenever possible

3. Sidestep Phishing Scams

How-To: Hovering over a sender's email address or a link in an email can help you see whether the address or URL looks legitimate, but it's easy to miss the subtle differences between a legit link or web address and a fraudulent one. To be safe, open a new browser tab and go to the company's website yourself—don't copy the link from the email! Then log in or call customer service to see what's going on with your account.

4. Update your software

Part 3: Your Digital Security Action Plan

5. Opt for extra protection
How-To: Install anti-virus software. Free AV software that CR recommends – Avira Free Security Suite and Kaspersky Security Cloud Free

6. Back Up Your Files

7. Encrypt Your Devices
How-To: In Windows 10, look under Settings for Update & Security, then Device encryption. Not there? On some Windows computers you'll need to search for Manage BitLocker instead— it allows you to choose specific files and folders to encrypt.

8. Rescue Lost Gadgets (Setup "Find My Device")

Part 3: Your Digital Security Action Plan

9. Safeguard Your WiFi

How-To: First, make sure you have strong passwords for your WiFi network and for controlling your router's settings. Next, ensure that the software for your router is always up to date. If the router is from your internet service provider, the company probably does that for you.

Once the manufacturer stops issuing updates, it's wise to get a new router.

10. Secure Security Cameras and Other Connected Gizmos

How-To: If you're shopping for an item such as a baby monitor, decide whether you really want one that connects to the internet. If you don't feel the need to check the monitor from your phone when you've left a babysitter in charge, consider a model that just works within your home. For items you do connect to WiFi, set up a strong password and use MFA if it's offered. Never use any default password that came with the device.