



## How to be cyber safe

Another day, another major data breach - or at least that's how it seems. The recent Equifax breach exposed the most confidential data of millions of users worldwide, perhaps the most serious leak to date. The Federal Trade Commission has compiled the [steps you should take in response to the Equifax breach](#), many of which are good security practices in any circumstances.

Data breaches by third parties are only one way that our financial data or identity can be stolen. Many tech experts say we are our own greatest threat by letting our guard down and not taking sufficient precautions. Digital privacy is vitally important. It is critical to be savvy about the many data-driven devices we use and the ways we communicate.

Here are things tech and security experts recommend that you do to stay safe:

- Secure your accounts by making passwords long, strong and unique. Avoid reusing passwords on your financial accounts.
- Update your browser, software and apps regularly.
- Use anti-virus software, a firewall and anti-spyware software. One method alone is insufficient.
- Back up your important documents, photos, and data frequently on an external hard drive or a cloud.
- Monitor your bank accounts, 401ks, brokerage, credit and debit card accounts regularly. Look for suspicious activity such as transactions you don't recognize and report any immediately.



- Get a free credit report annually from the three major credit bureaus at [annualcreditreport.com](http://annualcreditreport.com), the only federally authorized site for free reports.
- Be suspicious of any emails or phone calls with urgent requests for personal or financial information.
- Don't click links in an email, instant message or social media if the message looks suspicious. Instead, type the site address in your browser.
- Don't submit credit card or secure information on public WIFI. Never make a purchase on a site unless it is secure as indicated by the "s" in "https."
- Don't leave digital tracks. Avoid sharing personal or identifiable information on social media.
- File taxes early to minimize the risk of a third party intercepting your return. Remember, the IRS will never call you to demand immediate payment.
- Consider Identity Theft insurance.

Get more tips about online safety by logging in to your Member website at [www.HealthCareEAP.com](http://www.HealthCareEAP.com).