Cybersecurity for American Families

A 10-Step Data Security Guide for the People You Love
ABOUT THIS PROJECT

This guide was produced as part of Duke University’s Bass Connections program, in which research teams of students and faculty tackle complex societal problems. Our group, the “How Do Cyberattacks Hurt Us?” project team, studied data breaches and their impact on average Americans throughout the 2018-19 academic year.

For more information about how to protect your data, please visit our website at sites.duke.edu/10steps. The website provides additional user-friendly resources and an accessible version of this guide.

OUR TEAM

ANALESE BRIDGES
Trinity College of Arts and Sciences ’19
B.A. Political Science

MATTHEW PHILLIPS
Duke University School of Law ’20
Juris Doctor

SHREYA HURLI
Trinity College of Arts and Sciences ’21
B.S. Economics

SABRINA PIN
Trinity College of Arts and Sciences ’21
B.S. Computer Science

DAVID LIU
Pratt School of Engineering ’21
B.S.E. Electrical & Computer Engineering
B.S. Computer Science

MARY WANG
Trinity College of Arts and Sciences ’21
B.S. Economics

INTRODUCTION

Cybersecurity, simplified.

American families are spending more time online than ever before. We browse the internet, post to social media, buy products, send emails, and monitor our finances on an ever-expanding array of devices—from computers, smartphones, and tablets to internet-connected watches and smart speakers. It has never been easier to digitally manage almost any part of our personal and professional lives.

But the convenience of our connected world comes with a price. Bad actors can take advantage of security flaws in our devices to access sensitive personal information—our phone numbers, bank account information, social security numbers, and more. They use this information to steal our identities, allowing them to purchase goods or take out loans in our names. Sorting through the wreckage from a stolen identity is time-consuming and stressful, even when we don’t lose money in the end.

It is possible to protect ourselves and the people we love online—and it’s easier than you might imagine.

Preventing our information from getting into the wrong hands can sometimes seem complicated and overwhelming, but it does not have to be this way. Created with the insights of cybersecurity experts at Duke University and throughout the country, this guide includes ten easy and actionable steps that we can all take to secure our digital lives. It is possible to protect ourselves and the people we love online—and it’s easier than you might imagine.
STEP 1

Take control of your privacy.

You leave an information trail when you post on social media, visit a website, or use an app on your phone. It is sometimes possible for bad actors to purchase or steal this information and learn about your habits, what you like and dislike, and even where you go throughout the day.

Try to limit the information you share with third parties by reviewing and adjusting the privacy settings on the devices and apps you use. If you do not want your social media apps selling your location information, for example, you may have to toggle a switch within the app or in your mobile device settings to restrict the sharing of this data.

STEP 2

Find out where your data lives.

Most companies have privacy or data policy webpages specifying the types of information they collect and who can access this data. Reviewing these policies can help you decide whether you feel comfortable sharing your information with the companies. To find a company’s privacy or data policies, look for a link at the bottom of its website or within its app. Make sure you understand what the policies say, and remember that a company’s policies are only as good as its commitment to complying with them.

STEP 3

Keep your devices up-to-date.

If the software on your computer and mobile devices is out-of-date, bad actors may be able to take advantage of security flaws and access your information. Software updates often help fix these flaws, so you should update your software as frequently as possible. You can even enable automatic updates for some programs to ensure that you always have the latest and most secure versions on your devices.

For additional protection, consider installing antivirus and antispyware software on your computer and turning on your computer’s firewall. Antivirus software helps prevent attackers from using programs or code to alter the way your computer operates, and antispyware software helps prevent attackers from secretly collecting your personal information. A firewall blocks other attempts to access your device.
STEP 4

Be Wi-Fi wise.

When you connect to the internet using a Wi-Fi network that is not secure, cybercriminals may access the files stored on your computer or mobile device, track the websites you are visiting, and even copy your login information and passwords. Protect your information by requiring a password to log into your home Wi-Fi network.

Avoid using free, unsecured Wi-Fi networks, and only use trusted networks that are password-protected.

Be cautious when connecting to new Wi-Fi networks outside your home. Avoid using free, unsecured public Wi-Fi networks, and only use trusted networks that are password-protected. Disable the automatic Wi-Fi connection feature on all of your devices so that they do not connect to new, unsafe networks without your knowledge.

For greater protection outside your home, consider connecting to a virtual private network, or VPN. These services mask your identity and protect your data from bad actors. It is usually best to choose a VPN that charges a monthly or annual fee, as free options are generally less secure.

STEP 5

Create stronger passwords.

Simply changing your passwords can reduce your chances of being the victim of a cyberattack. Short, simple passwords with personal meaning are easy for hackers to crack, but longer passwords tend to be more secure. Try stringing together four unrelated but recognizable words, such as textbook-lightbulb-coupon-waterfall. This password is hard to decode because of its length, and it is far easier to remember than a random string of letters and numbers.

Use a different password for every website that you log into. Although no password is completely secure, a smart password strategy can prevent hackers from using the same password to access all of the information you store on different websites.

<table>
<thead>
<tr>
<th>PASSWORD</th>
<th>COMPARISON</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1</strong></td>
<td>Buddy123</td>
</tr>
<tr>
<td>PASSWORD STRENGTH</td>
<td>✅ ✅ ✅</td>
</tr>
<tr>
<td>This password is short and uses personal information (like the name of your dog). It is very easy for hackers to decode.</td>
<td></td>
</tr>
<tr>
<td><strong>2</strong></td>
<td>R3rtDIhnb=</td>
</tr>
<tr>
<td>PASSWORD STRENGTH</td>
<td>✅ ✅ ✅</td>
</tr>
<tr>
<td>This password is stronger because it contains a random mix of letters and numbers and does not include any personal information. However, it is still easy for hackers to decode because it is so short.</td>
<td></td>
</tr>
<tr>
<td><strong>3</strong></td>
<td>textbook-lightbulb-coupon-waterfall</td>
</tr>
<tr>
<td>PASSWORD STRENGTH</td>
<td>✅ ✅ ✅</td>
</tr>
<tr>
<td>This password is much more secure because it is so long. It is also easy to remember because it includes recognizable words.</td>
<td></td>
</tr>
</tbody>
</table>
**STEP 6**

**Take two steps.**

While using a strong password helps to protect your information, no password is entirely secure. That’s why it is important to take an additional step to prevent your data from getting into the wrong hands. By enabling two-factor authentication for your online accounts, you can make it harder for bad actors to log into the accounts—even if they know your password.

Two-factor authentication asks that you verify your identity after entering your password, such as by typing in a temporary code sent to your phone via text message. This requires very little extra effort on your part, but it acts as an additional bump in the road that bad actors will be less likely to traverse. Many online services and social media apps now offer this feature, and it is easy to set up. You can even choose to enable multi-factor authentication on some accounts, which provides even more protection.

**STEP 7**

**Avoid sharing sensitive information.**

Unless absolutely necessary, do not share sensitive information such as bank account information, credit card numbers, or social security numbers in emails or text messages—even if you trust the person or group receiving these messages. While your accounts may never be hacked, your friends’ and family members’ accounts could be—and you want to make sure that your sensitive information is not swept up in the process.

**STEP 8**

**Don’t be caught by phishing.**

Bad actors sometimes use a technique known as phishing to trick people into giving up their personal information. Phishing comes in many forms: you might receive a link in an email that takes you to a dangerous website hosted by bad actors, an attachment that contains malware, or even a phone call from an impersonator requesting your personal information.

With hundreds of millions of phishing attempts every year, it is important to be aware of the signs of a scam. Look for suspicious links that appear within pop-up windows, emails that ask you to verify or change your account number or password, and emails with typos. In general, if something doesn’t feel right, you shouldn’t click on a link, download a file, or share any personal information.
Get a free freeze.

If bad actors are able to steal your information, they may be able to access your bank accounts or take out loans in your name. A credit freeze makes it more challenging for them to do so by preventing banks and other companies from sharing your credit information.

You should get a credit freeze if you notice any unfamiliar transactions on your financial statements, such as your credit card bill or credit report. You can get a free freeze by contacting Equifax, Experian, and TransUnion, the three nationwide credit reporting agencies.

LOG ON
To get a free credit freeze, visit each of these websites and follow the steps provided:

1. Equifax: equifax.com/personal/credit-report-services
2. Experian: experian.com/freeze
3. Transunion: freeze.transunion.com

Make sure your elected officials protect your data, too.

Implementing the previous nine steps will help you and your family protect your information online, but the most effective protection isn’t possible without strong data privacy laws. To learn more about cybersecurity laws in your state, visit your state attorney general’s website. If you care about your data privacy, make sure you let your elected representatives know—every letter, email, and phone call can make a difference.
This project is part of Duke University’s Bass Connections program, in which research teams of students and faculty tackle complex societal problems.

ACKNOWLEDGMENTS
We are grateful to our team leaders, Sarah Bloom Raskin, Lee Reiners, and Meredith Edelman, for guiding us through this process, and to our project manager, Mokshada Mahajan, for providing administrative support. We also had the privilege of working on this project with several external consultants, who shared their expertise on cybersecurity law and policy, cyber hygiene, best practices, and more. Thank you to Shane Stansbury, Rochelle Newton, Sara Sternberg Greene, Kathleen Hamm, David Finn, Richard Biever, and Kody Kinsley.

sites.duke.edu/10steps