IDENTITY GUARD

5 Every Day Habits That Increase The Risk of Identity Theft

IDENTITY GUARD

At Identity Guard, we're constantly working to protect our members from evolving threats.

Over the 23 years that we've been protecting people's identities, we've learned that identity protection is not one size fits all. Because we're all different, our unique every day actions will affect the types of identity theft risk that we encounter.

We can't tell you how to live your life, but we can share with you some of what we've learned.

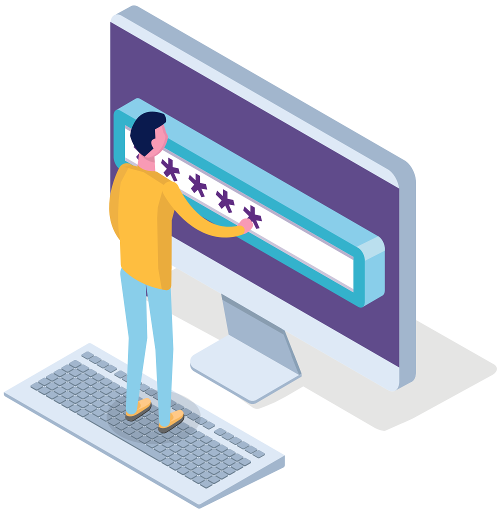
In this eBook, we've identified some of the most common habits that increase the risk of identity theft. Some may seem obvious or innocent, but all 5 are behaviors that are worth paying attention to in order to lead a more secure digital life.

1. SENDING SENSITIVE DATA VIA EMAIL OR MESSAGING

When was the last time that you walked away from your computer with the screen still on?

One of the hidden risks of online communication comes from messaging apps and emails. These tools make our lives infinitely easier: we send off important information to colleagues and friends in a matter of seconds.

But every email or message exists in two places: in the sender's account, and in the recipient's. You can take steps to limit your risk (set up two factor authentication, encrypt your messages, only send personal information to those that you know and trust via email) but no matter what precautions you take, your message may still end up exposed on the recipient's screen.

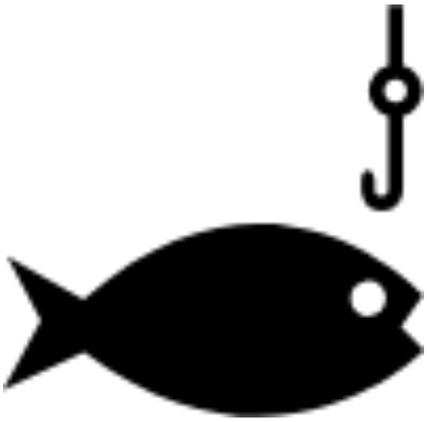


2. CHOOSING WEAK PASSWORDS

You live in the digital age, which means you've heard this one before. You *know* that each of your passwords should be unique, and you're also acutely aware of the uphill battle that is remembering unique passwords.

But there's a reason why warnings to use unique passwords are everywhere: passwords are the front door to your digital life. If someone can unlock the front door, they've got access to everything inside the house.

If there's one habit to break to increase your online security, then this is the one.



3. NOT RESEARCHING DATA RECIPIENTS

A second hidden risk of online communication? Identity thieves who present themselves as someone else, likely someone you know and trust, and ask for your personal information.

Known as "phishing", identity thieves are savvy. They're able to create emails that look like they've been sent from your boss and web pages that look identical to your online banking portal.

If you receive an email prompting you to respond with sensitive, personal data (log-in credentials, your Social Security number, your address, your birthdate) or to reset your password on any platform, make sure to investigate the email address or phone number that the message was sent from before responding.

The habit of not looking before you leap, or in this case, not investigating before you hit "send", could have substantial consequences.

4. NOT MONITORING ACCOUNTS OR CREDIT

Individuals who have no transaction alerts or warnings set up on their online accounts are not more likely to fall victim to identity theft, but they are more likely to have a hard time noticing that something illicit has happened.

Early detection is the key to stopping identity theft or fraud before it gets worse. By not monitoring your bank accounts or credit card statements, you put yourself at a considerable disadvantage when it comes to detection of fraud. You can compare this to buying a house and not installing smoke detectors.

Most credit cards have customizable settings that will allow you to request notifications to your smartphone when a purchase is made on your card. This is one of the simplest steps you can take to increase your security measures.

5. SHARING YOUR PERSONAL INFORMATION ON SOCIAL MEDIA

Facebook quizzes are fun. Slow days at work can often lead to curiosity about which character from *Friends* you are, or what your face swapped with your favorite celebrity's might look like. So what if you have to give a 3rd party application access to your profile information and friends list?

Plus, you know that you're a Chandler and will want to share the results with your friends once the quiz proves you right.

We don't tend to view this light hearted habit as detrimental, but factual information (your birthday, where you grew up, your maiden name or heritage) can easily be turned in to answers to your authentication questions when logging in to your most important accounts.

Social media is for sharing, but when it comes to what you share, use a discerning eye and do your best not to overshare.

Have these habits under control?

Sign up for Identity Guard today to find out what else you can do to help keep your identity protected.