KEATING WEALTH MANAGEMENT

Cybersecurity 101

Overview

Cybercrime is a serious threat. Attacks have multiplied with the deployment of more sophisticated phishing techniques and hacking software. One study found that identity fraud cost Americans around $56 billion in 2020.[1] Federal Trade Commission identity theft reports doubled from 2019.[2]

With vigilance and preventive measures, you can safeguard your information and wealth. Here, we outline a few simple actions you should take **today**.

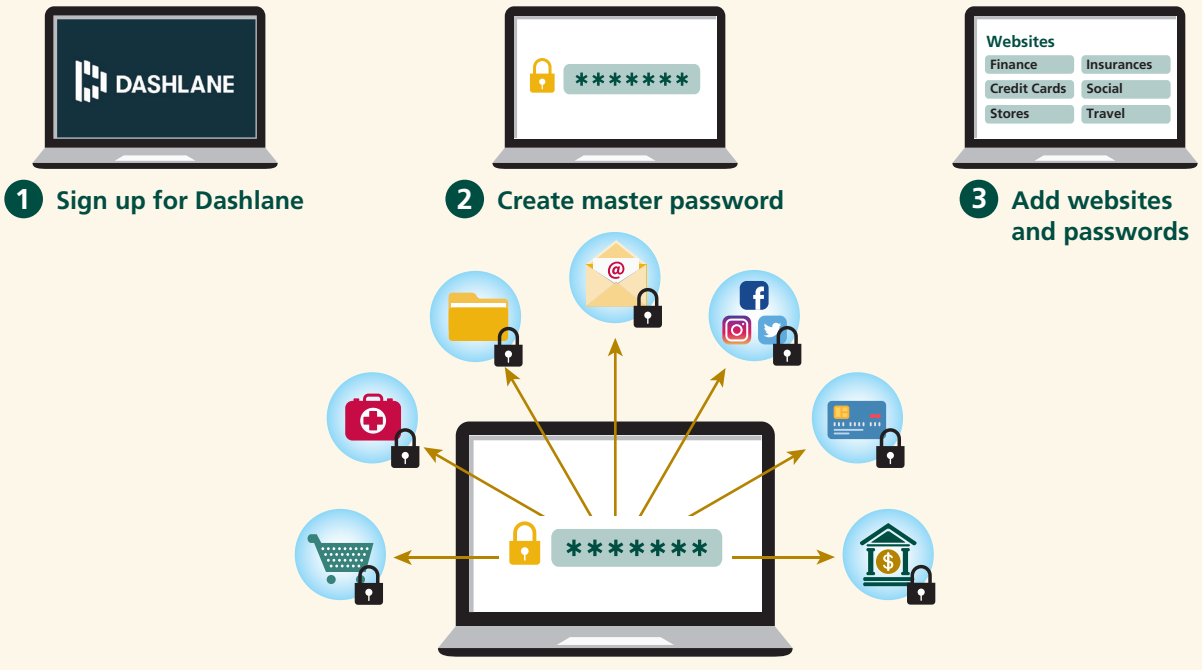
Password management software is your best friend

As we create ever more digital accounts, it becomes tempting to use the same password—or embarrassingly simple passwords—to secure our data. Hackers can recognize these patterns and easily crack them, so we need a better solution.

Password managers keep your information safe by encrypting your passwords in the cloud or on your computer. The software can generate a completely random password for each account, and it locks them all behind ***one master password*** that only you know.

You can use the same password manager across multiple devices, take advantage of convenient autofill functionality, and store security questions with your passwords. While it takes an initial investment of time and effort to set up, the advantages are innumerable. *Password managers are extremely secure and cannot view your passwords themselves.*

How Password Management Software Works



1 Sign up for Dashlane

2 Create master password

3 Add websites and passwords

4 Dashlane will log in with the passwords you have stored as you visit the applicable sites

[1] *https://www.cnbc.com/2021/03/23/consumers-lost-56-billion-dollars-to-identity-fraud-last-year.html*

[2] *https://www.ftc.gov/news-events/press-releases/2021/02/new-data-shows-ftc-received-2-2-million-fraud-reports-consumers*

Password management software makes your life easier. You get stronger passwords and don't have to remember them. Access is nearly instant, and you can relax knowing that even if one site has a data breach, the rest of your passwords are still safe.

DASHLANE

Dashlane is our password manager of choice. It's simple to set up: Just download your browser extension, provide an email address and master password, and it records your passwords as you go, avoiding the need to input all your passwords manually. Premium family plans start at $7.49 a month (as of July 2021).

Always turn on multifactor authentication

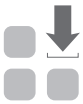
As hackers have gotten more sophisticated, your username and password combination alone may not be enough to protect your accounts. Attackers have become adept at guessing passwords from social media and exploiting massive data leaks. Luckily, turning on two-factor or multifactor authentication, when available, can act as a last line of defense.

Two-factor authentication adds an extra layer of security and comes in many different forms. The hope is that while hackers may have one piece of information about you, they are unlikely to have two, so your account is better protected.

Common forms of two-factor authentication

Hardware tokens are small physical devices, such as a fob that produces a code you must input before entering a site.

Text message or voice authentication sends a code via phone call or text that you need to input in order to log in.



Software tokens require you to download a multifactor authentication app to your phone to receive a code that typically expires after a short period of time—perhaps a minute—and allows you to log in.

Biometric tokens use fingerprints, retina scans or facial recognition to provide access.

A Verizon report found that stolen, reused and weak passwords are the leading cause of security breaches. Multifactor authentication, in conjunction with a password manager, is the best way to prevent your information from being stolen.[3]

Avoid phishing attacks

Phishing is a cybercrime where an attacker sends a fraudulent message—typically a phone call, text or email—designed to trick a victim into revealing sensitive information, such as a credit card number, password or Social Security number. Some emails may also embed malicious software or viruses to extract information from victims.

[3] *https://www.verizon.com/business/resources/reports/dbir/2021/masters-guide/*

For instance, an email might say your account is being deactivated and ask you to click a link or enter your password to restore it. You might receive a call saying your taxes were misfiled and that you must provide your Social Security number or else face fines or jail time. Stressed and nervous, millions of Americans fall prey to these scare tactics.

Luckily, phishing attacks are preventable. Never provide sensitive information on the phone or via email, and carefully check email addresses. An email from Facebook, for example, should contain an address that ends in @facebook.com, not a random string of letters and numbers, as is common in phishing attacks. Only click links and attachments from known senders, and hover over links to see where they lead.

Use comprehensive cybersecurity software

Besides protecting your passwords through two-factor authentication and password managers, full-service internet security suites can protect you and your family from elements out of your control. Norton AntiVirus uses common software signatures to identify viruses and warn users. It also provides email spam filtering and phishing protection.

Know what to do if you become a cybercrime victim

Despite all your preventive measures, you find unknown charges on your credit card. Or one of your minor children—the population most susceptible to cybercrime—falls for a phishing scheme. Always contact the local police. In some situations, you should also contact the FBI or FTC. Here are some common scenarios:

Hacked internet account

If you can no longer log into an account, try resetting your password and check that your email is still linked to the account. If this doesn't work, contact the company directly to regain access.

If you've used the hacked password for other accounts, change those passwords immediately. Verify that no purchases or posts were made on the hacked account, and alert friends and family that you've been hacked, as attackers often take advantage of your contacts when they gain access to your account.

Stolen identity

If your identity is stolen (for example, via your Social Security number or credit card information), you have the right to place fraud alerts on your credit report, which tells creditors they must verify who is applying for credit in your name. You should also immediately report this crime to the FTC. Under most state laws, you bear no responsibility for debt incurred on accounts fraudulently opened in your name. Under federal law, you're liable for $50 at most when a thief uses a stolen credit card—$0 if you report the theft quickly.

You should immediately report a debit card loss to your bank or credit union, as there is a higher potential for liability.

If you report your debit card lost:	Your maximum loss is:[4]
Before any unauthorized charges are made	$0
Within 2 business days after learning about the loss or theft	$50
More than 2 business days after the loss or theft, but fewer than 60 calendar days after statement is sent to you	$500
Over 60 calendar days after your statement is sent to you	Possibly unlimited

Identity theft prevention software may put a freeze or lock on your credit after an identity crime. Both block access to your credit history, helping you control account openings in your name and guarding against identity theft. However, there are some differences between the two.

Credit locks are must faster to set up and manage than a freeze, though agencies may charge a fee. You can instantly activate and deactivate a lock.

Credit freezes may take up to 24 hours to remove. They also block ***authorized*** access to credit information, preventing you from getting instant credit when you need it.

Software such as LifeLock can recognize breaches, help you freeze or lock your credit, send fraud alerts to protect you, and aid in recoup losses.

Conclusion

In today's digital world, there's nothing you can do to prevent cybercrime. But you can take simple steps to protect yourself and your family from the most common attacks. Our biggest recommendation is to ***take action today***. Using even one of the tools discussed—multifactor authentication, a password manager, or comprehensive antivirus software—is far better than doing nothing.

[4] *https://www.identitytheft.gov/#/Know-Your-Rights*

July 2021

KEATING WEALTH MANAGEMENT

www.keatingwealth.com
(720) 408-5250