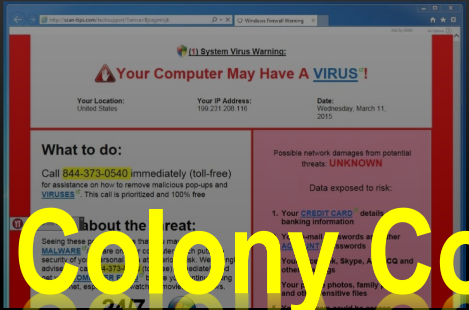


(1) System Virus Warning:

Your Computer May Have A VIRUS!

Your Location: United States

Your IP Address: 199.231.208.116

Date: Wednesday, March 11, 2015

What to do:

Call 844-373-0540 immediately (toll-free) for assistance on how to remove malicious pop-ups and VIRUSES. This call is prioritized and 100% free

Possible network damages from potential threats: UNKNOWN

Data exposed to risk:

1. Your CREDIT CARD details banking information

Fords Colony Computer & Technology Club

Combatting Scam Phone Calls

& Scam/Junk/Phishing Emails

& Password Managers

May 15, 2023

On March 10, 1876
Alexander Graham Bell
makes the first Phone call ever…

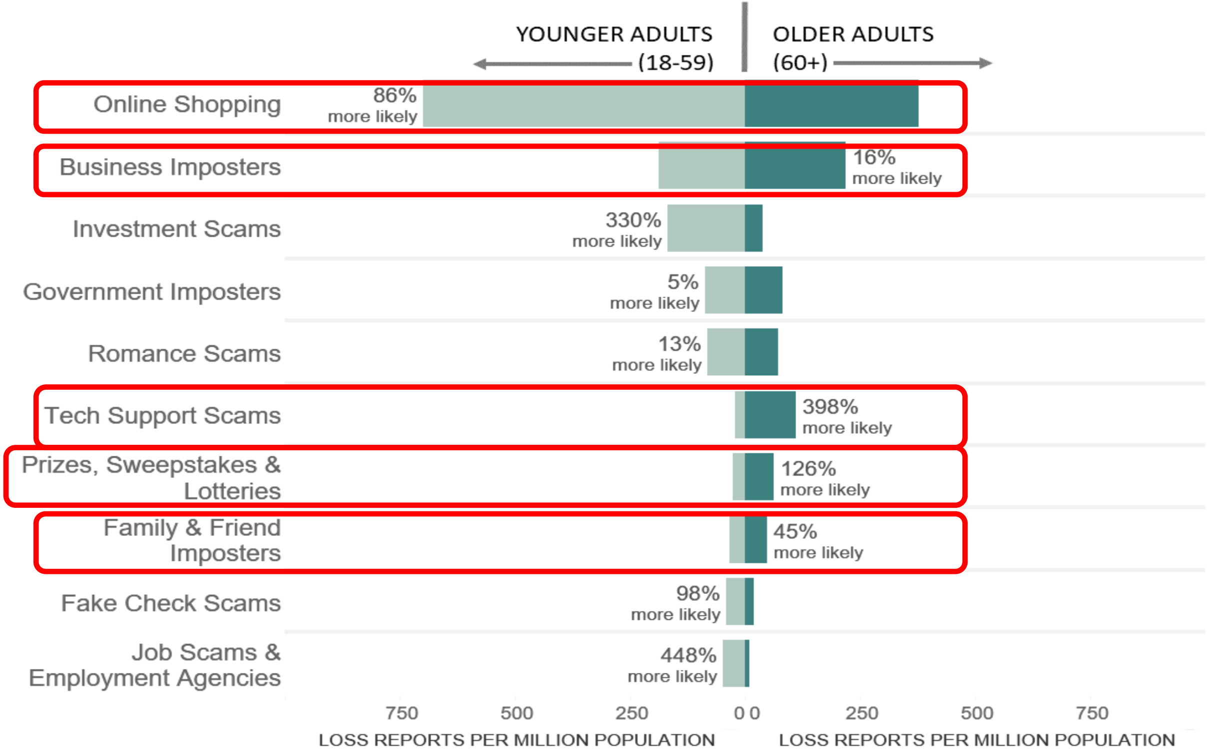
And moments later he was notified that his car’s extended warranty had expired…

SCAMS – FTC VIDEO

https://www.youtube.com/watch?v=MUA0wtZVX8E&t=0s

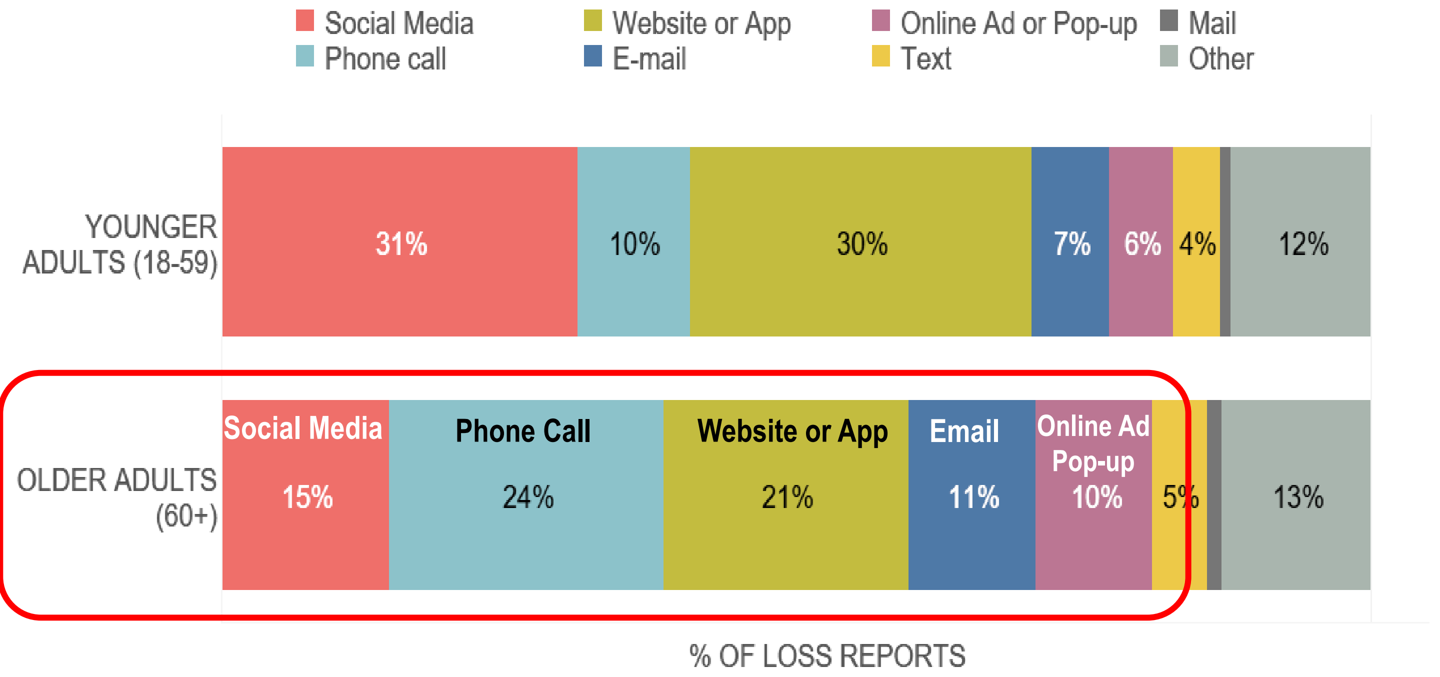
2021 LOSS REPORTS BY AGE AND FRAUD TYPE

Losses to some types of fraud are more likely to be reported by younger adults, while others are more likely to be reported by older adults.



Figures are normalized using U.S. Census Bureau data for population by age. See U.S. Census Bureau, Annual Estimates of the Resident Population for Selected Age Groups by Sex for the United States (June 2020). Reports categorized as unspecified and reports provided by IC3 are excluded.

2021 FRAUD CONTACT METHODS BY AGE AND SHARE OF LOSS REPORTS

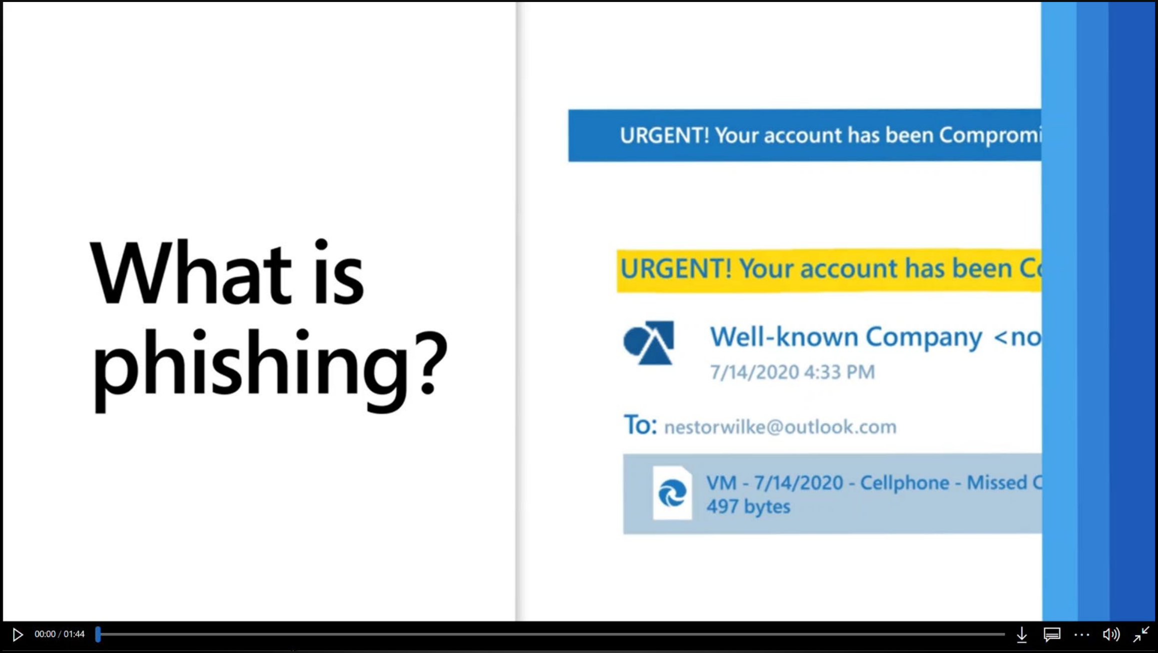


Figures are based on fraud reports to the FTC's Consumer Sentinel Network that indicated a dollar loss, including reports provided by data contributors. Reports without age and contact method data are excluded from percentage calculations.

SCAM & FRAUD TOPIC DEFINITIONS

Term	Definition
Junk/SPAM Email	Email spam, also referred to as junk email, spam mail, or simply spam, is unsolicited messages sent in bulk by email (spamming). Most email spam messages are commercial in nature. Whether commercial or not, many are not only annoying as a form of attention theft, but also dangerous because they may contain links that lead to phishing web sites or sites that are hosting malware or include malware as file attachments.
Malware	Malware (malicious software) is any software intentionally designed to cause disruption to a computer, server, client, or computer network, leak private information, gain unauthorized access to information or systems, deprive access to information, or which unknowingly interferes with the user's computer security and privacy. The defense strategies against malware differ according to the type of malware but most can be thwarted by installing antivirus software, firewalls, applying regular patches to reduce zero-day attacks, securing networks from intrusion, having regular backups and isolating infected systems.
Phishing	Phishing is a form of social engineering where attackers deceive people into revealing sensitive information or installing malware such as ransomware. Phishing attacks have become increasingly sophisticated and often transparently mirror the site being targeted, allowing the attacker to observe everything while the victim is navigating the site, and transverse any additional security boundaries with the victim. As of 2020, it is the most common type of cybercrime, with the FBI's Internet Crime Complaint Centre reporting more incidents of phishing than any other type of computer crime.
Pop-Up Ads/Messages	Pop-up ads or pop-ups are forms of online advertising on the World Wide Web. A pop-up is a graphical user interface (GUI) display area, usually a small window, that suddenly appears ("pops up") in the foreground of the visual interface. They can also be generated by other vulnerabilities/security holes in browser security.

WHAT IS PHISHING?



What is phishing?

URGENT! Your account has been Compromi

URGENT! Your account has been C

Well-known Company <no

7/14/2020 4:33 PM

To: nestorwilke@outlook.com

VM - 7/14/2020 - Cellphone - Missed C

497 bytes

https://www.youtube.com/watch?v=YfiN_W8I1cE

SCAM & FRAUD TOPIC DEFINITIONS

Term	Definition
Call blocking	Call blocking, also known as call block, call screening, or call rejection, allows a telephone subscriber to block incoming calls from specific telephone numbers. This feature may require an additional payment to the subscriber's telephone company or a third-party.
Caller ID Spoofing	Caller ID spoofing is the practice of causing the telephone network to indicate to the receiver of a call that the originator of the call is a station other than the true originating station. This can lead to a caller ID display showing a phone number different from that of the telephone from which the call was placed.
Robocalls	A robocall is a phone call that uses a computerized autodialer to deliver a pre-recorded message, as if from a robot. Robocalls are often associated with political and telemarketing phone campaigns but can also be used for public service or emergency announcements. The service is also associated to be prone to scams.
Email filtering (host systems)	A feature of most email hosting services to allow wanted email; to be received in the Inbox and unwanted email to be redirected automatically to the Junk or SPAM folder. Hosting services use algorithms to perform this task, but they are sometimes prone to filter out legitimate email.
Email filtering - whitelisting & blacklisting	An ***enhanced*** feature of many email hosting services (via webmail) and some email clients (Outlook, etc.) to increase the accuracy of email filtering. Used most often to correct the host system filtering. For example, if a legitimate email is being sent to Junk/SPAM or an illegitimate email is being sent to the Inbox – the end user can override the filtering classifications going forward.

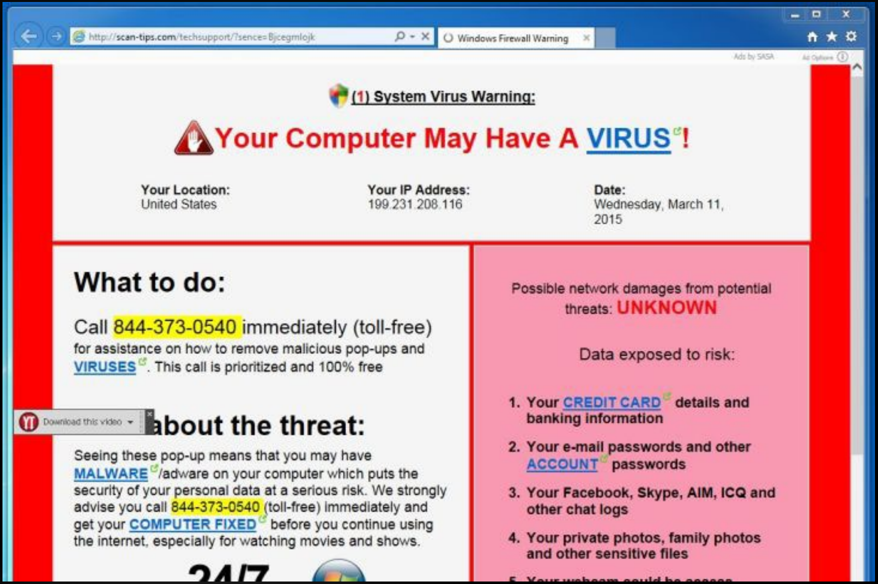
WHAT IS MALWARE?

Protect your devices and data from malware

https://support.microsoft.com/en-us/windows/how-malware-can-infect-your-pc-872bf025-623d-735d-1033-ea4d456fb76b

WHAT'S A POP-UP?

- Pop-up ads or pop-ups are forms of online advertising on the World Wide Web. A pop-up is a graphical user interface (GUI) display area, usually a small window, that suddenly appears ("pops up") in the foreground of the visual interface. They can also be generated by other vulnerabilities/security holes in browser security.



(1) System Virus Warning:

Your Computer May Have A VIRUS!

Your Location:
United States

Your IP Address:
199.231.208.116

Date:
Wednesday, March 11, 2015

What to do:

Call 844-373-0540 immediately (toll-free) for assistance on how to remove malicious pop-ups and VIRUSES. This call is prioritized and 100% free

about the threat:

Seeing these pop-up means that you may have MALWARE/adware on your computer which puts the security of your personal data at a serious risk. We strongly advise you call 844-373-0540 (toll-free) immediately and get your COMPUTER FIXED before you continue using the internet, especially for watching movies and shows.

24/7

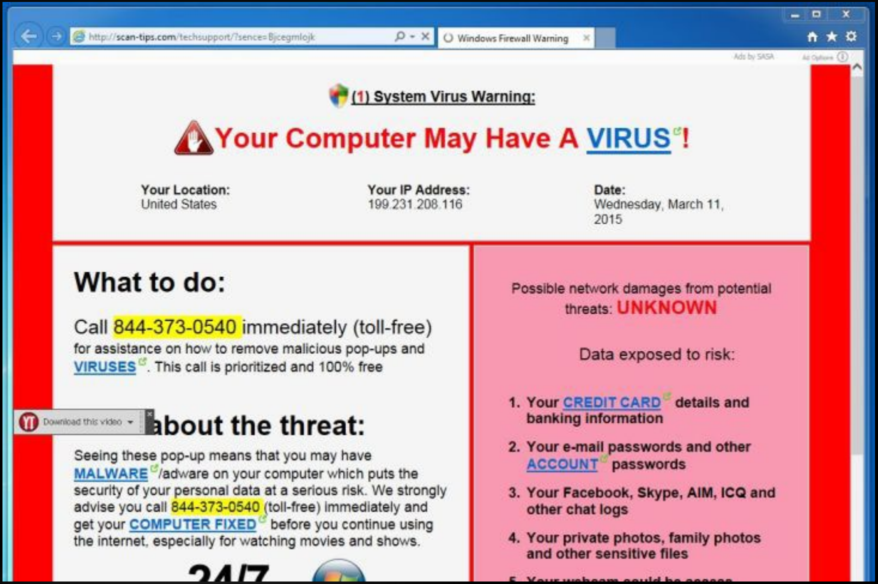
Possible network damages from potential threats: UNKNOWN

Data exposed to risk:

1. Your CREDIT CARD details and banking information
2. Your e-mail passwords and other ACCOUNT passwords
3. Your Facebook, Skype, AIM, ICQ and other chat logs
4. Your private photos, family photos and other sensitive files
5. Your webcam could be access

MORE ABOUT POP-UPS

- Perpetrators (perps) often smuggle pop-ups riding hidden in email, use easily mis-spelled web addresses, hijacking friend and family address books.
- Perps and their confederates often sell or share email addresses as potential targets.
- Often, they prey on your fears and encourage you to take ***immediate*** action telling you that your failure to act ***NOW*** will result in something bad for you.



(1) System Virus Warning:

Your Computer May Have A VIRUS!

Your Location:
United States

Your IP Address:
199.231.208.116

Date:
Wednesday, March 11, 2015

What to do:

Call 844-373-0540 immediately (toll-free)
for assistance on how to remove malicious pop-ups and VIRUSES. This call is prioritized and 100% free

about the threat:

Seeing these pop-up means that you may have MALWARE/adware on your computer which puts the security of your personal data at a serious risk. We strongly advise you call 844-373-0540 (toll-free) immediately and get your COMPUTER FIXED before you continue using the internet, especially for watching movies and shows.

24/7

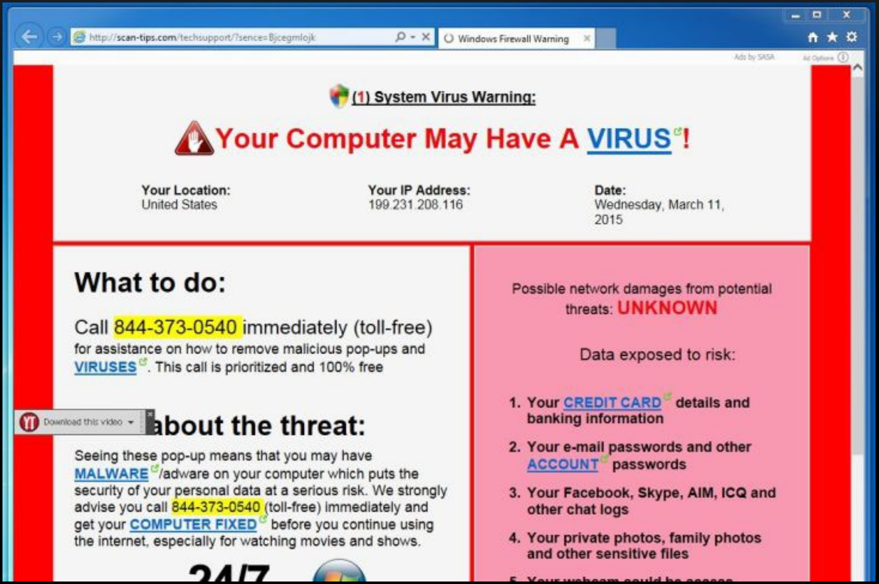
Possible network damages from potential threats: **UNKNOWN**

Data exposed to risk:

1. **Your CREDIT CARD details and banking information**
2. **Your e-mail passwords and other ACCOUNT passwords**
3. **Your Facebook, Skype, AIM, ICQ and other chat logs**
4. **Your private photos, family photos and other sensitive files**
5. **Your webcam could be access**

WHAT TO DO WHEN YOU GET A POP-UP

- Take a deep breath and calm down!
- **Don't call their phone number or tap or click on any hyper-link!**
- If the pop-up is a web page in your browser, delete/close that browser page.
- If the pop-up ins in its own window – recommend powering down your device, then power it back up. If pop-up doesn't reappear – you're good to go!
- If it reappears after power cycling, you may need additional help.
- See article below for more tips.



http://scan-tips.com/techsupport/?sence=Bjcegmlojk

Windows Firewall Warning

(1) System Virus Warning:

Your Computer May Have A VIRUS!

Your Location: United States

Your IP Address: 199.231.208.116

Date: Wednesday, March 11, 2015

What to do:

Call 844-373-0540 immediately (toll-free) for assistance on how to remove malicious pop-ups and VIRUSES. This call is prioritized and 100% free

about the threat:

Seeing these pop-up means that you may have MALWARE/adware on your computer which puts the security of your personal data at a serious risk. We strongly advise you call 844-373-0540 (toll-free) immediately and get your COMPUTER FIXED before you continue using the internet, especially for watching movies and shows.

24/7

Possible network damages from potential threats: UNKNOWN

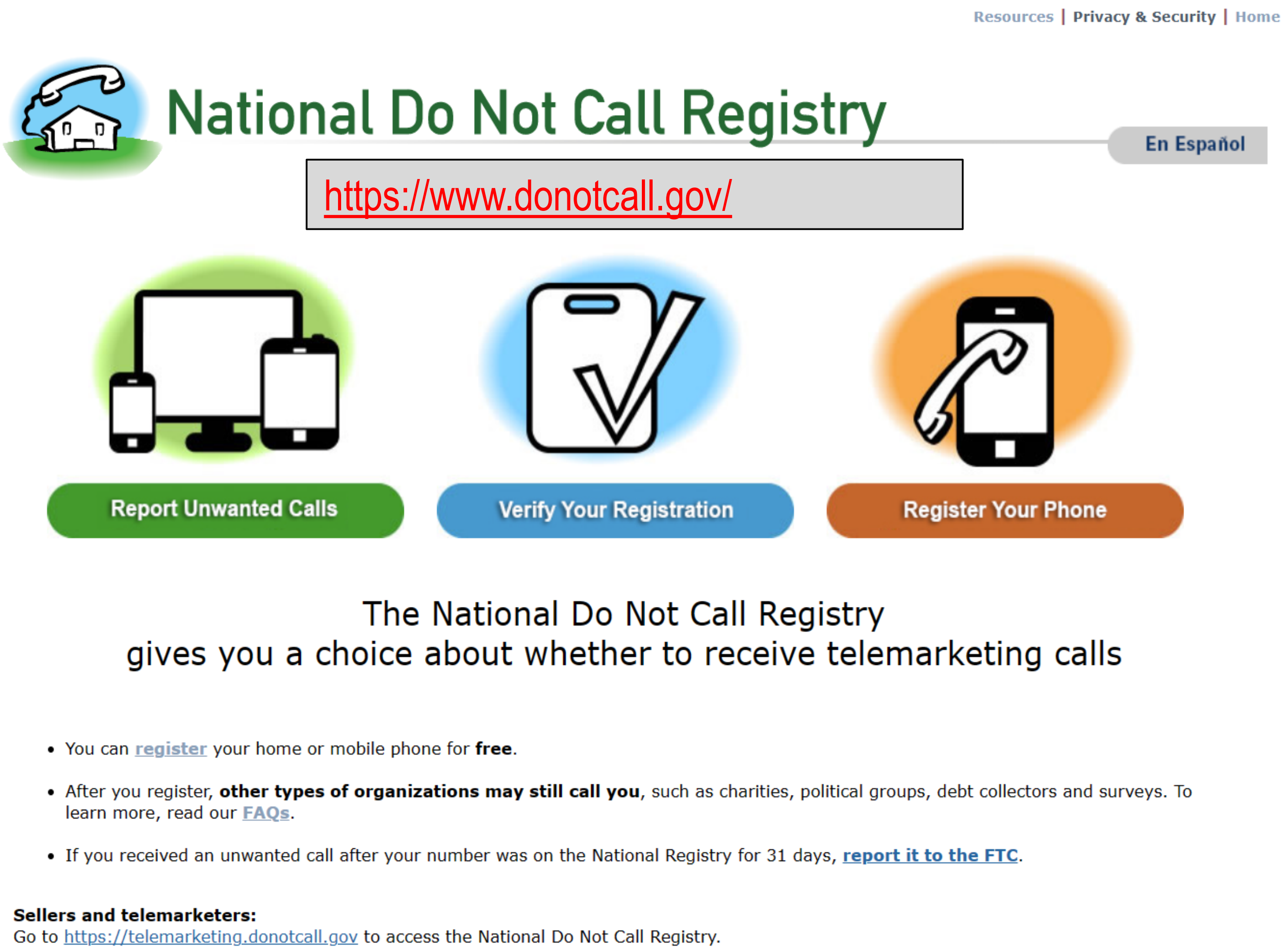
Data exposed to risk:

1. Your CREDIT CARD details and banking information
2. Your e-mail passwords and other ACCOUNT passwords
3. Your Facebook, Skype, AIM, ICQ and other chat logs
4. Your private photos, family photos and other sensitive files
5. Your webcam could be access

https://www.wikihow.com/Close-an-Internet-Pop-Up

PHONE SCAM CALL TACTICS

- Be suspicious of **<u>all</u>** incoming calls from unknown persons or alleged organizations
- Be suspicious of **<u>all</u>** incoming calls from an organization or company, that you have done business with, allegedly advising you of a serious issue with your account, etc.
  - Hang up and call them back on a legitimate phone number
  - Don’t trust Caller ID – perps can and do spoof the displayed information
- Register your phone number(s) with the ***National Do Not Call Registry***



National Do Not Call Registry

https://www.donotcall.gov/

The National Do Not Call Registry gives you a choice about whether to receive telemarketing calls

- You can register your home or mobile phone for **free**.
- After you register, **other types of organizations may still call you**, such as charities, political groups, debt collectors and surveys. To learn more, read our FAQs.
- If you received an unwanted call after your number was on the National Registry for 31 days, **report it to the FTC**.

Sellers and telemarketers:
Go to https://telemarketing.donotcall.gov to access the National Do Not Call Registry.

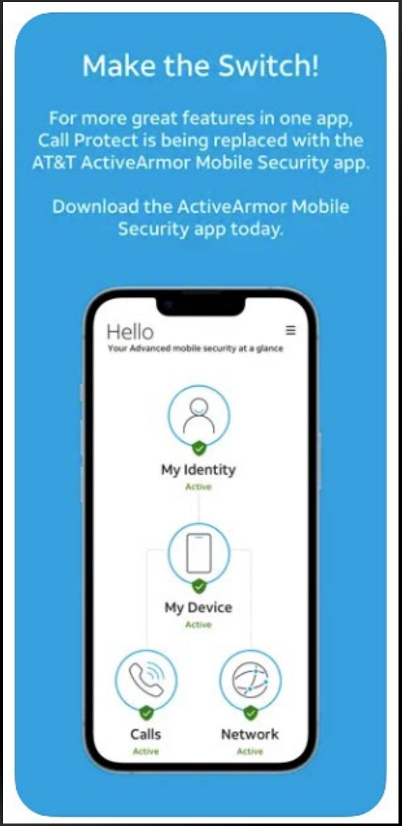
MOBILE PHONE SCAM CALL PREVENTION TACTICS

- Populate your mobile phone’s address book (or Contacts) with family, friends, businesses, organizations, etc.
- Most smartphones have privacy settings:
  - Adjust which calls you will allow to come through
  - Block specific numbers
- Most cellular service providers offer optional services to block robocalls, SPAM calls, etc. Some are free; some have fees.
- 3rd Party Applications - Robokiller, NoMoRobocall, etc.

AT&T CALL PROTECT

AT&T ActiveArmorSM Key Features and Benefits include*:

- Auto Fraud Call Blocking: Detects and blocks calls from likely fraudsters before they reach you.
- Spam Risk Call Blocking: Blocks or sends calls to voicemail if identified as Spam Risk.
- Nuisance Call Alerts: Labels potential nuisance calls from telemarketers, surveys, and more.
- Nuisance Call Controls: Choose call categories to accept, block, or send to voicemail.
- Unknown Calls to Voicemail: Automatically sends callers to voicemail if they are not in your address book and blocks other numbers in your personal block list.
- Personal Block List: Add individual unwanted callers to your own block list.
- Device Security: Helps protect your data from mobile threats.
- Breach Report Alerts: Informs you about corporate data breaches.



Make the Switch!

For more great features in one app, Call Protect is being replaced with the AT&T ActiveArmor Mobile Security app.

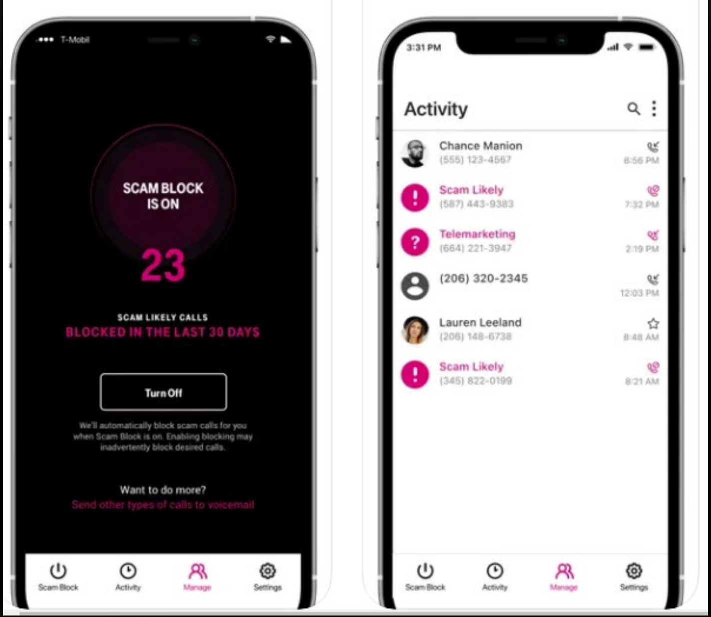
Download the ActiveArmor Mobile Security app today.

T-MOBILE SCAM SHIELD

Scam Shield gives you control over T-Mobile's anti-scam protections like Scam ID, Scam Block, and Caller ID, and is available to all our customers.

ADVANCED NETWORK TECHNOLOGY - Our supercharged network analyzes every call using A.I., machine learning, and patented technologies. And our defenses update every six minutes to stay ahead of scammers.

- Scam Block – Our network will automatically block calls from likely scammers, when you turn it on, helping to keep them off your phone entirely.
- Scam Reporting – Help identify suspicious callers or fraudsters and prevent their calls from being received by you—or others—in the future.
- Caller ID – See who's calling before you answer.
- Allow list – Calls from numbers on your Allow list will never be blocked by our network and always ring your phone.
- Personal Number Blocking – Block specific numbers and contacts as soon as they hit the T-Mobile network.
- Category Manager – Tired of telemarketers? Or survey calls? We'll identify and block call types you don't want to see anymore.
- Reverse Number Lookup – Not sure who a number belongs to? We'll do a reverse phone number lookup and show you anything we can about who is calling.
- Voicemail to Text - Get text messages containing readouts of blocked calls that were sent to voicemail



SCAM LIKELY CALLS BLOCKED IN THE LAST 30 DAYS

We'll automatically block scam calls for you when Scam Block is on. Enabling blocking may inadvertently block desired calls.

Want to do more?
Send other types of calls to voicemail

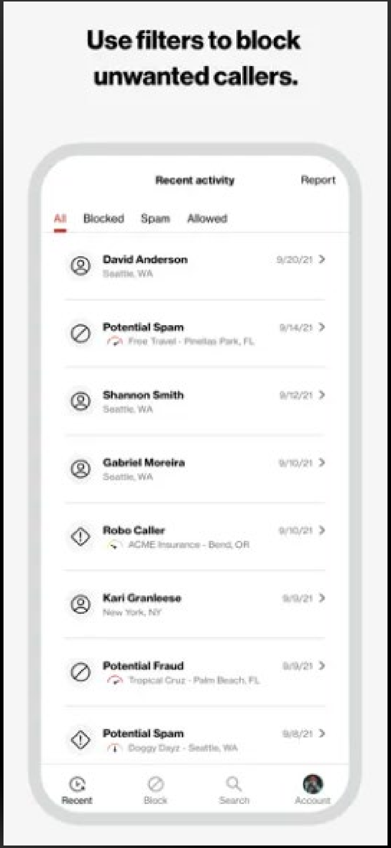
Chance Manion (555) 123-4567	8:56 PM
Scam Likely (587) 443-9383	7:32 PM
Telemarketing (664) 221-3947	2:19 PM
(206) 320-2345	12:03 PM
Lauren Leeland (206) 148-6738	8:48 AM
Scam Likely (345) 822-0199	8:21 AM

VERIZON CALL FILTER

Verizon Call Filter takes the guesswork out of answering your phone, with features that screen and automatically block incoming spam calls.

With Call Filter, you can:

- Identify suspected spam calls with alerts.
- Automatically block spam based on their risk level and send them to voicemail (Call Filter automatically blocks high-risk callers).
- Report phone numbers as spam.
- Use filters to block other unwanted callers, such as robocalls.
- Adjust spam filter settings any time.
- For added security, upgrade to Call Filter Plus*. Features such as Caller ID and blocking entire area codes give you even more control over incoming calls.



Use filters to block unwanted callers.

Recent activity

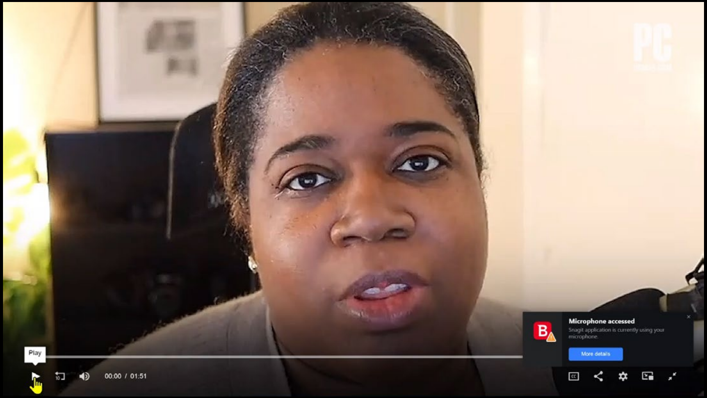
David Anderson	Seattle, WA	9/20/21
Potential Spam	Free Travel - Pinellas Park, FL	9/14/21
Shannon Smith	Seattle, WA	9/12/21
Gabriel Moreira	Seattle, WA	9/10/21
Robo Caller	ACME Insurance - Bend, OR	9/10/21
Kari Granleese	New York, NY	9/9/21
Potential Fraud	Tropical Cruz - Palm Beach, FL	9/9/21
Potential Spam	Doggy Dayz - Seattle, WA	9/8/21

MALWARE & VIRUS PREVENTION TACTICS

1. Install Anti-Virus on your computers
   - Also strongly encourage Anti-Virus/Web Protection for tablets and smartphones
2. Keep your Anti-Virus up to date
   - Periodically perform a full (deep) anti-virus scan of your devices
   - Perform a full scan if you think you may have been infected
3. Always keep the operating systems (OS’s) on your computers, tablets and smartphone updated
   - Windows, MacOSX, Android, iPadOS, iOS
4. Don’t tap or click on any attachments or hyperlinks in email from an unknown source – delete them!
5. Reveal the true Email Addresses

PASSWORD MANAGERS

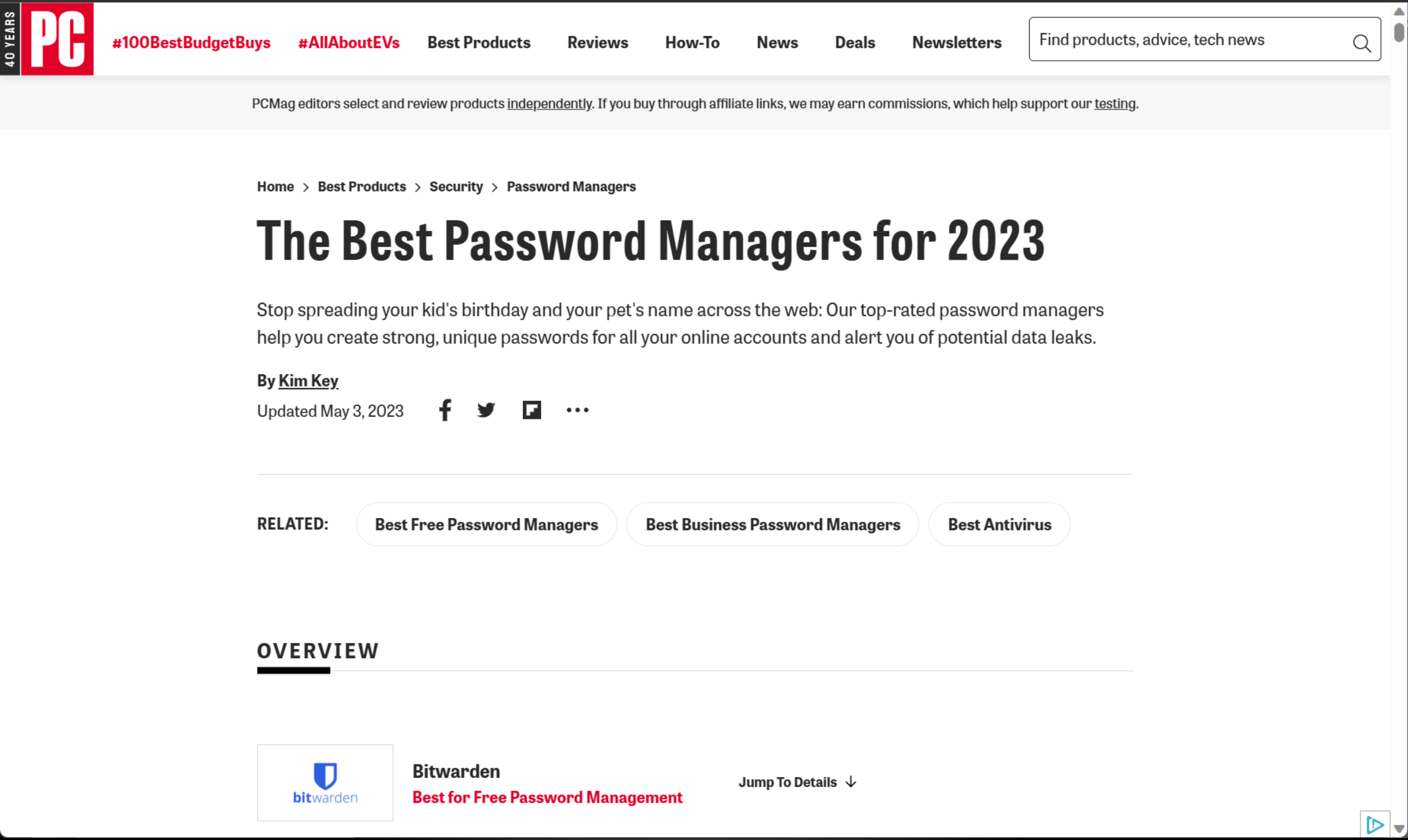
- A password manager is a software application designed to securely store and manage passwords and other sensitive information, such as login credentials, credit card details, and personal information.
- Password managers generate and store unique, complex passwords for each online account, eliminating the need to remember multiple passwords.
- Users can access their passwords and other sensitive information through a master password, which is the only password they need to remember.
- Password managers typically use encryption and other security measures to protect user data and prevent unauthorized access.
- Using a password manager can improve security and convenience for online accounts.



Microphone accessed

Snagit application is currently using your microphone.

https://www.pcmag.com/picks/the-best-password-managers



PCMag editors select and review products independently. If you buy through affiliate links, we may earn commissions, which help support our testing.

Home > Best Products > Security > Password Managers

The Best Password Managers for 2023

Stop spreading your kid's birthday and your pet's name across the web: Our top-rated password managers help you create strong, unique passwords for all your online accounts and alert you of potential data leaks.

By Kim Key

Updated May 3, 2023

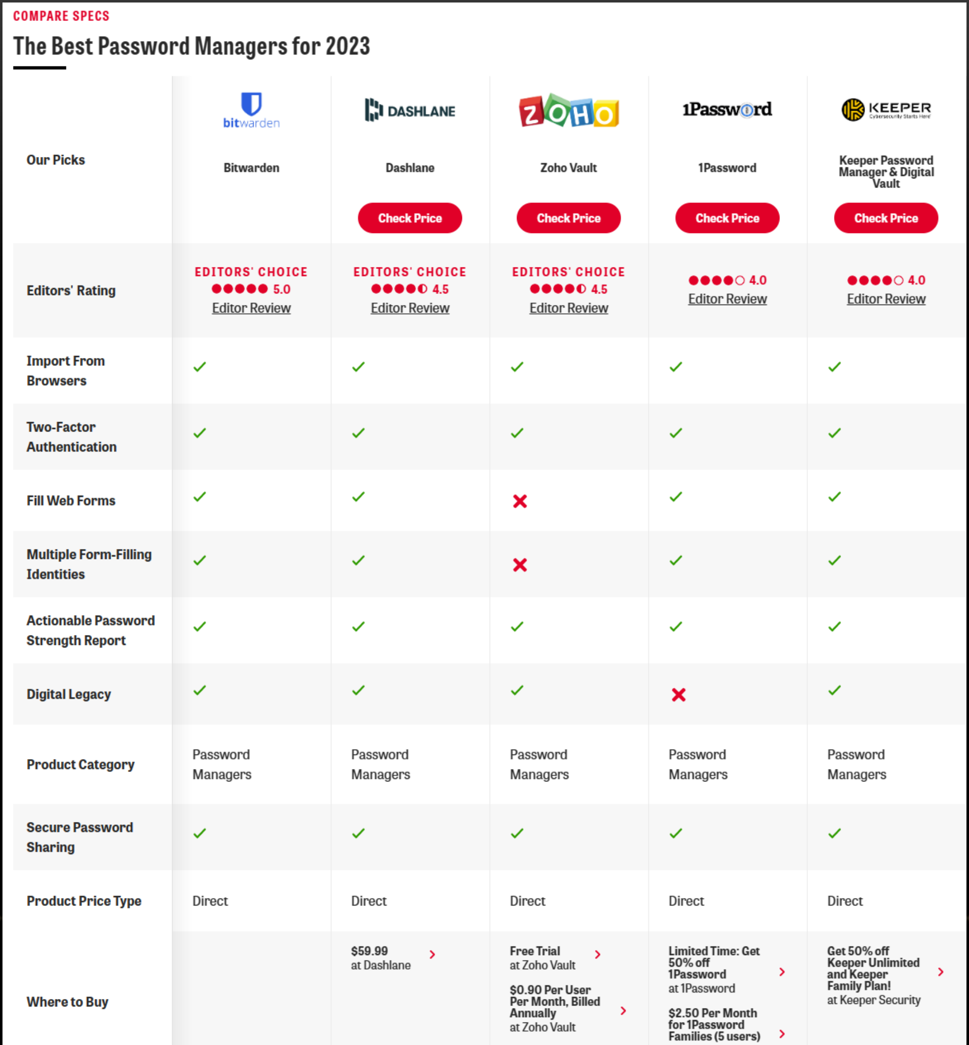
RELATED: Best Free Password Managers | Best Business Password Managers | Best Antivirus

OVERVIEW

Bitwarden

Best for Free Password Management

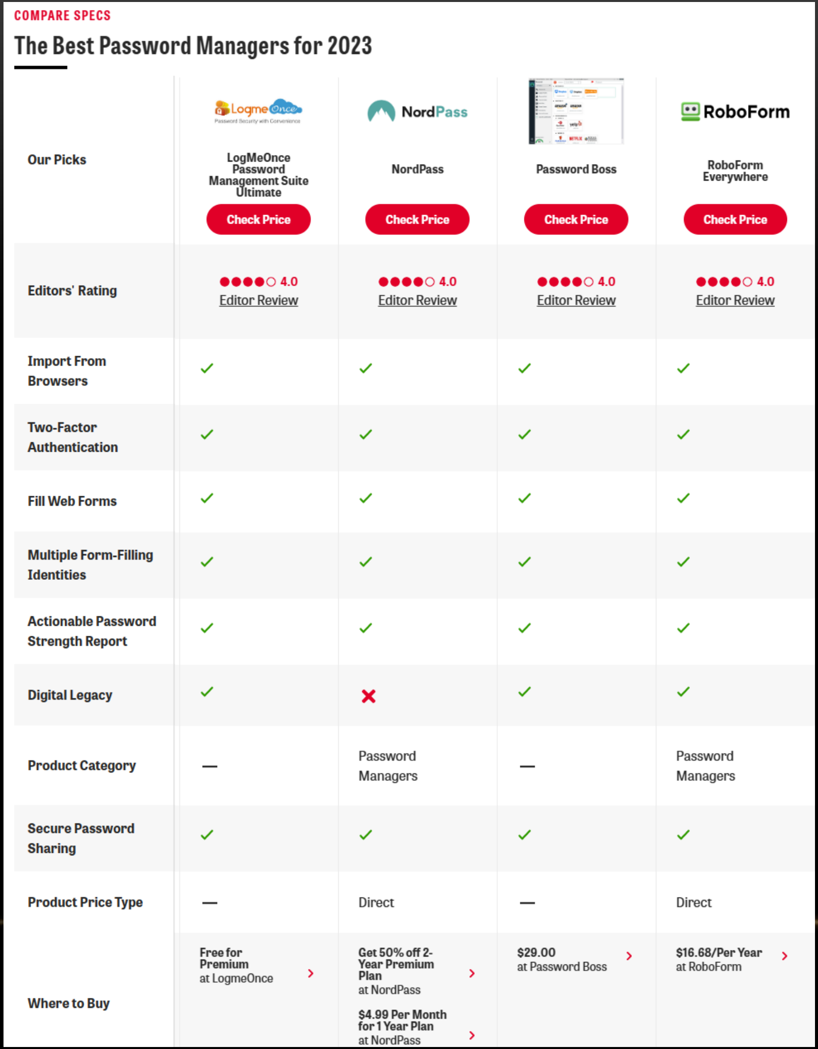
https://www.pcmag.com/picks/the-best-password-managers



COMPARE SPECS

The Best Password Managers for 2023

Our Picks	Bitwarden	Dashlane Check Price	Zoho Vault Check Price	1Password Check Price	Keeper Password Manager & Digital Vault Check Price
Editors' Rating	EDITORS' CHOICE ●●●●● 5.0 Editor Review	EDITORS' CHOICE ●●●●◐ 4.5 Editor Review	EDITORS' CHOICE ●●●●◐ 4.5 Editor Review	●●●●○ 4.0 Editor Review	●●●●○ 4.0 Editor Review
Import From Browsers	✓	✓	✓	✓	✓
Two-Factor Authentication	✓	✓	✓	✓	✓
Fill Web Forms	✓	✓	✗	✓	✓
Multiple Form-Filling Identities	✓	✓	✗	✓	✓
Actionable Password Strength Report	✓	✓	✓	✓	✓
Digital Legacy	✓	✓	✓	✗	✓
Product Category	Password Managers	Password Managers	Password Managers	Password Managers	Password Managers
Secure Password Sharing	✓	✓	✓	✓	✓
Product Price Type	Direct	Direct	Direct	Direct	Direct
Where to Buy		$59.99 at Dashlane ›	Free Trial at Zoho Vault › $0.90 Per User Per Month, Billed Annually at Zoho Vault ›	Limited Time: Get 50% off 1Password at 1Password › $2.50 Per Month for 1Password Families (5 users) ›	Get 50% off Keeper Unlimited and Keeper Family Plan! at Keeper Security ›



COMPARE SPECS

The Best Password Managers for 2023

Our Picks	LogMeOnce Password Management Suite Ultimate	NordPass	Password Boss	RoboForm Everywhere
	Check Price	Check Price	Check Price	Check Price
Editors' Rating	●●●●○ 4.0 Editor Review	●●●●○ 4.0 Editor Review	●●●●○ 4.0 Editor Review	●●●●○ 4.0 Editor Review
Import From Browsers	✓	✓	✓	✓
Two-Factor Authentication	✓	✓	✓	✓
Fill Web Forms	✓	✓	✓	✓
Multiple Form-Filling Identities	✓	✓	✓	✓
Actionable Password Strength Report	✓	✓	✓	✓
Digital Legacy	✓	✗	✓	✓
Product Category	—	Password Managers	—	Password Managers
Secure Password Sharing	✓	✓	✓	✓
Product Price Type	—	Direct	—	Direct
Where to Buy	Free for Premium at LogmeOnce ›	Get 50% off 2-Year Premium Plan at NordPass › $4.99 Per Month for 1 Year Plan at NordPass ›	$29.00 at Password Boss ›	$16.68/Per Year at RoboForm ›

PASSWORD MANAGERS

PROS ✓

- Enhanced security: Password managers can help you create complex and unique passwords for each of your accounts, which can help protect you from password-related attacks like brute force attacks and password reuse attacks.
- Convenience: You only need to remember one master password to access all your other passwords, which can save you time and hassle.
- Automatic form filling: Password managers can also automatically fill in forms with your login credentials, which can be especially convenient if you have to log in frequently to the same websites.
- Cross-platform support: Password managers are typically available on multiple platforms, including desktops, smartphones, and tablets, so you can access your passwords from anywhere.
- Encrypted storage: Most password managers use encryption to store your passwords, which makes it difficult for hackers to access your data.

CONS

- Single point of failure: If someone gains access to your master password, they can access all your other passwords, which could be a major security risk.
- Cost: While many password managers are free or offer basic plans for free, more advanced features often require a paid subscription.
- Password manager compatibility: Not all websites and applications are compatible with all password managers, which can make using them more complicated.
- Dependency on the password manager: If your password manager fails for any reason, you may not be able to access your passwords.
- Initial setup: Setting up a password manager can take some time, especially if you have many different passwords to import.