TASKFORCE

NOVEMBER 2026 EDITION

YOUR IDENTITY.
YOUR MONEY.
YOUR LIFE.



THE AMERICAN'S DIGITAL SURVIVAL GUIDE

Protect your identity. Cut the spam.
Stop paying for what you forgot.

ENTERPRISE SECURITY THINKING.
BUILT FOR YOUR PERSONAL LIFE.

FREE EXPOSURE SCAN. INSTANT RESULTS.

GETTASKFORCE.COM/SCAN

Results appear when the scan completes. Timing varies.

READ IT. USE IT. SHARE IT.

YOUR PERSONAL SECURITY BRIEFING

The risks are connected. Your protection should be, too.

03 A message to every American
04 Our mission
05 The threat, by the numbers
06 How your exposure spreads
07 This is happening right now
08 12 common scams to recognize
09 Why your phone keeps ringing
10 The subscriptions you forgot
11 Who is exposed?
12 What is really at stake
13 The cost of doing nothing
14 Seven moves to make today
15 Where single tools fall short
16 The Task Force protection system
17 Protection that keeps working
18 Put your money back on watch
19 One life. Several lines of defense.
20 Choose your protection
21 Answers and an emergency plan
22 Sources and methodology
23 Product notes and sources
24 Run your free exposure scan

Start with what is exposed. Then put protection to work.

YOU SHOULD NOT NEED AN IT DEPARTMENT TO FEEL SAFE.

A MESSAGE TO EVERY AMERICAN

You lock your front door. Who is watching the doors into your digital life?

Your phone number travels. Your address appears in databases. Old passwords survive in breach files. Meanwhile, subscriptions renew whether you remember them or not.

You can be careful and still be exposed. A company you trusted can lose your information. A caller can sound official. A charge small enough to miss can repeat for years.

The FBI recorded $20.9 billion in reported internet-crime losses in 2025, up 26% from 2024. The problem is bigger than an annoying call. It can reach your savings, your accounts and the people who trust you. [1]

This guide shows you where the risks connect, what you can do today and how Task Force brings ongoing privacy, identity and money protection into one place.

You do not have to watch every database and every bill yourself. But leaving your exposure unchecked gives problems more time to develop.

Take the next few minutes seriously. Start by finding out what is already exposed.

[1] FBI IC3, 2025 data. Full source links and measurement notes on pages 22-23.

PERSONAL SECURITY DESERVES A SERIOUS SYSTEM.

OUR MISSION.
YOUR PEACE OF MIND.

ENTERPRISE SECURITY THINKING.

Reduce exposure. Watch for warning signs. Respond when something changes. Keep checking. That discipline belongs in your personal life, too.

1 LESS OF YOU FOR SALE

Find exposed personal records and request their removal from supported people-search and data broker sites.

2 MORE VISIBILITY INTO RISK

Watch registered information for signs of exposure and receive alerts that help you decide what to do next.

3 MORE CONTROL OVER YOUR MONEY

Bring recurring charges into view so you can spot waste, choose what stays and cancel what no longer earns its place.

Task Force works in the background so protection does not become another full-time job.

Services and automation depend on your plan, activation and linked accounts. [10-15]

ORDINARY INFORMATION. EXTRAORDINARY CONSEQUENCES.

THE THREAT, BY THE NUMBERS

~23 SEC

ONE IDENTITY THEFT REPORT

Approximate average interval between identity theft reports to the FTC network in 2025. [2]

$20.9B

REPORTED INTERNET-CRIME LOSSES

FBI IC3 recorded 26% more reported losses in 2025 than in 2024. [1]

1.75B

SCAM + TELEMARKETING ROBOCALLS

YouMail estimated this many U.S. calls in October 2026 alone. [3]

59.9%

PAYING FOR SOMETHING UNUSED

Share of respondents reporting an unused paid subscription in Self Financial's 2026 survey. [4]

These measure different things: reports, losses, estimated calls and survey responses. They are not your personal odds of becoming a victim.

[1-4] Periods and definitions matter. The 23-second figure is an annualized approximation, not a count of unique victims.

THE ATTACK CAN BEGIN LONG BEFORE THE CALL.

HOW YOUR EXPOSURE SPREADS

A name, a number and a familiar detail can make a stranger sound like someone you should trust.

DATA IS COLLECTED

Public records, online forms and exposed account information can reveal pieces of your life.

DETAILS ARE CONNECTED

People-search profiles can connect your address, phone number, age and relatives.

THE APPROACH FEELS PERSONAL

An imposter uses those details to give a call, text or message a sense of legitimacy.

URGENCY TAKES OVER

A threat, fake security alert or urgent request pushes you to act before you verify.

Less public exposure means fewer personal details to weaponize.

Illustrative risk pathway, not a claim that every listing leads to fraud. [5, 6, 10]

REAL WARNINGS. REAL ENFORCEMENT. RECENT EVENTS.

THIS IS HAPPENING RIGHT NOW.

JULY 20, 2026 / FBI WARNING

THE FAKE RESCUER

The FBI warned that scammers were impersonating IC3 personnel, using AI-generated videos and fake reporting sites to target people who had already lost money. [5]

Your takeaway: verify a recovery offer independently. A convincing video is not proof.

SEPTEMBER 17, 2026 / FBI WARNING

THE FAKE GOVERNMENT OFFICIAL

Nearly 61,000 complaints and more than $1.6 billion in losses were tied to government or law-enforcement impersonation from January 2025 through July 2026. [6]

Your takeaway: end the call and contact the agency through its official website.

SEPTEMBER 2026 / FTC UPDATE

THE SUBSCRIPTION THAT WOULD NOT GO

The FTC announced expanded refunds under the Amazon Prime settlement over alleged deceptive enrollment and cancellation practices. More than $845 million had been refunded by September 2026. [7]

Your takeaway: audit recurring charges and keep cancellation confirmations.

Sources [5-7]. Agency reports and allegations are attributed; these are not Task Force customer stories.

PAUSE. VERIFY INDEPENDENTLY. NEVER PAY UNDER PRESSURE.

12 COMMON SCAMS. KNOW THE PLAYBOOK.

FAKE BANK ALERTS

A fraud warning asks for codes or a transfer to a safe account.

Call your bank directly.

DELIVERY + TOLL TEXTS

An urgent fee or delivery problem links to a payment page.

Check the official site yourself.

GOVERNMENT IMPOSTERS

An IRS, police or agency caller threatens arrest or a fine.

Hang up. Verify with the agency.

AI FAMILY EMERGENCIES

A familiar voice needs cash now and asks you to keep it secret.

Call family on a known number.

TECH SUPPORT + REFUNDS

A virus alert or renewal notice asks you to call or grant access.

Use the vendor's official support.

JOB + TASK SCAMS

Easy online work requires a deposit to unlock your earnings.

Never pay to get paid.

ROMANCE + WRONG NUMBERS

A new online connection builds trust, then asks for money.

Do not send money to that contact.

INVESTMENT + CRYPTO

Guaranteed returns turn into fees to release your profits.

Stop. Verify independently.

FAKE SHOPS + SEARCH ADS

A bargain ad leads to an imitation store or payment site.

Check the seller and web address.

FAKE CHECK OVERPAYMENTS

A buyer or employer sends too much and wants money back.

Do not refund a stranger's check.

CHARITY + PRIZE IMPOSTERS

A familiar charity name or prize is used to demand a fee.

Verify charities. Prizes are free.

RECOVERY SCAMS

Someone promises to recover stolen money for an upfront fee.

Reject guaranteed-recovery offers.

Never share a sign-in code with an unexpected caller. A visible check deposit does not mean the check is genuine.

Tap a scam title for its FTC or FBI source. Common examples, not an exhaustive list. Report fraud at ReportFraud.ftc.gov. Guidance checked November 25, 2026.

A RINGTONE SHOULD NOT BE AN INVITATION TO STEAL.

YOUR PHONE NUMBER IS A TARGET.

4 BILLION+

Estimated U.S. robocalls in October 2026.
About 1,502 calls every second. [3]

The number on your screen is not proof of who is calling.

1 **THE SCALE**

YouMail estimated 1.75 billion scam and telemarketing robocalls in October. Not all robocalls are unwanted; reminders and notifications are also included in the total. [3]

2 **THE TACTIC**

Imposters can spoof familiar numbers and use urgent threats to keep you on the phone. Knowing your address does not make a caller legitimate. [6]

3 **THE TASK FORCE RESPONSE**

Data removal targets broker listings that can feed unwanted contact. Complete adds phone-spoofing and voice-phishing alerts. [11]

When a caller demands money, a code or remote access: stop. Call the organization through a number you already trust.

[3] Total robocalls rose 4.7% month over month; scam + telemarketing calls fell 0.6%. The longer-term total trend was downward. Removal cannot stop every call.

YOUR ATTENTION MOVED ON. THE BILLING DID NOT.

THE CHARGES YOU STOPPED SEEING.

59.9%

of respondents reported an unused paid subscription in a March 2026 survey for Self Financial. [4]

A free trial converts. A price rises. Two apps do the same job. An annual renewal lands on a card you rarely check. Each one is easy to miss on its own.

WHAT THREE FORGOTTEN CHARGES CAN COST

Unused streaming service	**$19.99 / month**
Duplicate cloud storage	**$9.99 / month**
Old fitness app	**$14.99 / month**

$539.64 **PER YEAR**

Illustrative arithmetic: $44.97 x 12. These are example charges, not average customer savings.

Task Force helps reveal recurring charges and supports cancellation of the ones you choose. [12]

[4] Survey of 1,272 U.S. adults; usage/cost questions were limited to paid subscribers. Unused means not used in the preceding 30 days.

BEING CAREFUL HELPS. IT DOES NOT ERASE YOUR RECORDS.

WHO IS EXPOSED?
PEOPLE WITH A LIFE.

1 WORKING PROFESSIONALS

Personal email, work contacts and a public profile can give an imposter material for a targeted approach.

2 PARENTS AND CAREGIVERS

Family details can make a fake emergency sound personal. Agree on a way to verify urgent requests.

3 ONLINE SHOPPERS

Every account creates another login to secure and another place to check for unfamiliar charges.

4 HOMEOWNERS AND MOVERS

Public addresses can linger after a move. Review what people-search sites reveal about your household.

5 SUBSCRIBERS AND APP USERS

Small recurring bills spread across cards and app stores can quietly escape attention.

6 RETIREES AND OLDER ADULTS

The FBI recorded $7.75 billion in reported internet-crime losses among people 60 and older in 2025. [1]

Different people face different levels of risk. These are common exposure situations, not predictions. [1, 5, 6, 10]

THE LOSS IS NOT ALWAYS JUST MONEY.

WHAT IS REALLY AT STAKE.

YOUR SAVINGS

A fake security emergency can turn into a payment you never intended to make.

YOUR ACCOUNTS

A stolen password can put email, shopping or financial accounts within reach.

YOUR IDENTITY

Misused personal details can lead to accounts or records you must dispute.

YOUR TIME

Calls, documentation and follow-up can compete with work and family.

YOUR MONTHLY CASH FLOW

Recurring charges keep taking money until the billing actually stops.



Risks described are possible consequences, not guaranteed outcomes. [1, 5, 6, 8, 9]

IGNORING A PROBLEM DOES NOT INTERRUPT IT.

DO NOTHING.
THE EXPOSURE STAYS.

You may never experience identity theft. But an exposed listing, reused password or unwanted subscription does not fix itself.

TODAY

Your information remains searchable. A reused password remains a weak point. The next renewal is still scheduled.

NEXT BILLING CYCLE

Charges you did not review can repeat. An alert you overlooked may remain unresolved.

AFTER ANOTHER DATA UPDATE

A removed broker listing may return when a site acquires new records. A one-time cleanup can go stale.

IF SOMETHING GOES WRONG

You may need to secure accounts, contact institutions, document losses and repair inaccurate records.

The reason to act is simple: close the gaps before you need the recovery plan.

Illustrative progression, not a forecast or guaranteed timeline. Broker re-listing and plan cadences: [10, 13].

KEEP THIS PAGE. START WITH THE FIRST UNCHECKED BOX.

SEVEN MOVES TO MAKE TODAY.

☐ 1 LOCK DOWN YOUR MAIN EMAIL

Use a long, unique password and a password manager. Your inbox is often the gateway to account resets.

☐ 2 TURN ON STRONGER SIGN-IN

Enable two-factor authentication. Prefer an authenticator app or security key where available.

☐ 3 UPDATE YOUR DEVICES

Turn on automatic updates for operating systems, browsers and apps. Keep security software current.

☐ 4 VERIFY BEFORE YOU ACT

Do not use links or callback numbers in unexpected messages. Open the official app or website yourself.

☐ 5 FREEZE YOUR CREDIT

Contact Equifax, Experian and TransUnion directly. Freezes are free and help restrict new credit in your name.

☐ 6 AUDIT RECURRING PAYMENTS

Review statements and app-store subscriptions. Mark each charge keep, cancel or investigate.

☐ 7 FIND YOUR PUBLIC EXPOSURE

Run the Task Force scan. Review the findings and decide whether ongoing removal and monitoring fit your needs.

Practical guidance: FTC account-security and credit-freeze resources [8, 9]. A freeze does not stop misuse of existing accounts.

USEFUL TOOLS WORK BEST WHEN THEIR GAPS ARE COVERED.

ONE TOOL.
ONLY PART OF THE JOB.

THE TOOL	THE LIMIT
CALL FILTERING Helps screen unwanted calls.	Does not remove all broker listings or audit your subscriptions.
PASSWORD MANAGER Helps create and store unique logins.	Does not remove your address from people-search sites.
CREDIT FREEZE Helps restrict new credit accounts.	Does not stop every scam or misuse of existing accounts.
ONE-TIME DATA REMOVAL Can reduce current public listings.	Needs follow-up because information can be re-listed.
SUBSCRIPTION TRACKER Helps surface recurring payments.	Does not resolve identity exposure or replace account security.

Keep the good habits. Add ongoing protection across the gaps.

Category-level comparison, not a rating of any named competitor. Task Force complements device security and credit freezes. [8-13]

THE TASK FORCE APPROACH: REDUCE, DETECT, RESPOND.

ONE PERSONAL PROTECTION SYSTEM.

Different services cover different points of failure. Together, they give you more ways to see and address a problem.

REDUCE EXPOSURE

Data removal

Find supported broker listings and request removal. Ongoing plans revisit the sites.

WATCH FOR MISUSE

Dark web + identity monitoring

Check registered identifiers for exposure and monitor supported identity signals.

FOLLOW THE MONEY

Subscription Manager

Surface recurring charges, price changes and duplicates in linked accounts.

HELP WITH RECOVERY

White-glove restoration

Complete members can work with a named specialist on identity-theft recovery.

Spam defense connects to data removal. Credit and financial alerts add visibility. Restoration supports the response if identity theft occurs.

Feature availability varies by plan. No service prevents every scam or identity theft. [10-15]

ONGOING PROTECTION NEEDS MORE THAN A ONE-TIME CHECK.

YOU LIVE YOUR LIFE. TASK FORCE KEEPS WATCH.

ALWAYS ON, WITH A CLEAR CADENCE.

Activated monitoring continues in the background. Broker rescans follow your plan schedule. Alerts and restoration support still require your attention when action is needed.

1 AT SETUP

Add the identifiers you want watched and activate available features. Link supported accounts for subscription visibility.

2 IN THE BACKGROUND

Dark web monitoring checks supported sources for registered information and alerts you to detected exposure.

3 AT THE NEXT RESCAN

Complete revisits 400+ broker sites monthly. Plus uses quarterly rescans across an expanded list.

4 WHEN SOMETHING CHANGES

Review the alert, verify it in your account and take the recommended steps. Use restoration support if needed.

Removal is a process: broker responses commonly take 7-45 days. Listings can reappear, which is why follow-up matters.

Essential has one-time guided removal. Monitoring is not a guarantee of immediate detection or complete source coverage. [10, 13, 14]

SUBSCRIPTION MANAGER | PLUS AND COMPLETE

YOUR MONEY DESERVES A WATCHDOG.

1 CONNECT ONCE

Link supported financial accounts through a read-only connection. Task Force says it never sees or stores your bank login.

2 SEE WHAT KEEPS RENEWING

Review recurring payments together. Look for duplicate services, price changes and charges you no longer recognize.

3 CHOOSE WHAT GOES

You decide what to cancel. Task Force helps with the process and tracks confirmation. Some merchants still require a call or an extra step.

YOUR 10-MINUTE MONEY CHECK

Would I buy this again today?
Is someone else in my household already paying for it?
Did I receive confirmation that cancellation is complete?

Complete also includes a budget, cash-flow and net-worth view through Money Plan.

Connected accounts and merchant requirements affect visibility and cancellation. Savings vary and are not guaranteed. [12, 15]

ILLUSTRATIVE EXAMPLE, NOT A CUSTOMER TESTIMONIAL.

ONE ORDINARY DAY. SEVERAL LINES OF DEFENSE.

THE PHONE RINGS

A caller knows your old address and claims to be from your bank.

Your move: hang up and call the bank directly.

Task Force role: reduce supported public listings; Complete adds spoofing and voice-phishing alerts.

AN EXPOSURE ALERT ARRIVES

An email or registered identifier is detected in supported breach data.

Your move: secure the affected account and any reused passwords.

Task Force role: bring detected exposure to your attention so you can respond.

THE MONTHLY REVIEW TAKES MINUTES

You notice an old app and a duplicate service among recurring charges.

Your move: decide what you no longer need.

Task Force role: organize linked-account subscriptions and help track cancellation.

Examples illustrate intended uses, not verified outcomes. Detection, removal and savings are not guaranteed. [10-15]

PUBLISHED INDIVIDUAL MONTHLY PLANS | NOVEMBER 25, 2026

CHOOSE YOUR LEVEL OF PROTECTION.

ESSENTIAL

Start with the basics.

$9.99 / MONTH

Guided removal from 10 sites, once.
Basic dark web monitoring.
Quarterly one-bureau credit score/report.

PLUS

Keep cleaning. Find forgotten charges.

$14.99 / MONTH

Quarterly automated broker rescans.
Subscription Manager.
Up to $1M identity theft insurance.

COMPLETE

Our broadest personal protection.

$39.99 / MONTH

Monthly rescans across 400+ sites.
Premium monitoring and restoration.
Subscription Manager + Money Plan.
Up to $5M identity theft insurance.

Monthly billing. Cancel anytime. Start with the free scan before choosing a plan.

Insurance subject to terms, conditions and exclusions; limits are not promised payouts. Published pricing/features may change. See gettaskforce.com/pricing. [13]

KNOW WHAT PROTECTION DOES, AND WHAT YOU STILL CONTROL.

STRAIGHT ANSWERS. A CLEAR NEXT STEP.

IS THE EXPOSURE SCAN REALLY FREE?

Yes. No credit card is required. The scan shows findings; paid plans provide removal and other protection features.

DOES A CLEAN SCAN MEAN I AM SAFE?

No. It reflects what that scan found in supported sources. It is not a complete audit of every account, device or database.

CAN EVERYTHING BE REMOVED?

No. Removal results depend on the source. Dark web monitoring alerts you to detected exposure; it does not erase leaked records.

WILL ALL CALLS STOP OR EVERY BILL DISAPPEAR?

No. Data removal may reduce exposure, and subscription tools help you act on selected charges. Results vary.

IF YOU THINK YOU HAVE BEEN SCAMMED

1. Stop contact. Call your bank or payment provider immediately.
2. Secure affected accounts and preserve messages and receipts.
3. Report identity theft at IdentityTheft.gov and internet crime at IC3.gov.
4. Contact Task Force through your account for available recovery help.

For immediate danger, call 911. Do not pay someone who promises guaranteed recovery. [5, 8, 9, 14, 16]

SOURCE NOTES | ACCESSED NOVEMBER 25, 2026

THE FACTS BEHIND THE BRIEFING.

1 FBI IC3: 2025 crime statistics

2025 losses: $20.877B, rounded to $20.9B; up 26%. Age 60+ losses: $7.749B, rounded to $7.75B. Complaint data, not all U.S. crime.

OPEN SOURCE

2 FTC: Protecting Older Consumers 2025-2026

October 19, 2026, p. 19: nearly 1.4M identity theft reports across Sentinel in 2025. Roughly 31,536,000 seconds / 1,400,000 = 22.5 seconds, rounded to about 23. Reports are not unique victims.

OPEN SOURCE

3 YouMail: October 2026 Robocall Index release

November 10, 2026: 4B+ total; 1,502/second; 1.75B scam + telemarketing. Estimates extrapolated from YouMail traffic. Total +4.7% month over month; unwanted category -0.6%; longer-term total trend downward.

OPEN SOURCE

4 Self Financial: unused subscriptions, 2026

March survey: 1,272 U.S. adults; 59.9% reported unused paid subscriptions. Usage/cost questions applied to paid subscribers; unused = no use in 30 days. Survey result, not a universal rate.

OPEN SOURCE

5 FBI: scammers impersonating IC3

July 20, 2026. Warning documents AI-generated videos, spoofed reporting sites and recovery schemes that target previous victims.

OPEN SOURCE

6 FBI: government and law-enforcement imposters

September 17, 2026. Nearly 61,000 complaints and more than $1.6B in losses, January 2025-July 2026. Includes spoofed contact details and AI-assisted impersonation.

OPEN SOURCE

7 FTC: expanded Amazon Prime refunds

September 2026 update to the 2025 settlement. More than $845M refunded by September. Settlement resolved allegations about enrollment and cancellation practices.

OPEN SOURCE

Click OPEN SOURCE to read the original. Figures from different reporting systems should not be added together.

WHAT THE SERVICE DOES. WHAT THE CLAIMS MEAN.

PRODUCT NOTES AND SOURCE LINKS.

8 FTC: account security and recovery
9 FTC: credit freezes and fraud alerts
10 Task Force: data removal
11 Task Force: spam and scam defense
12 Task Force: Subscription Manager
13 Task Force: plans, cadences and insurance
14 Task Force: dark web monitoring
15 Task Force: security and account linking
16 Task Force: free scan and restoration

RESTORATION DETAILS

Protection scope. Features require an active eligible plan and relevant setup. Sources and supported accounts vary. Task Force does not guarantee prevention, immediate detection, removal from every source or recovery of every loss. It complements secure devices, strong sign-ins and safe decisions.

Always on. Refers to activated ongoing monitoring. Broker removal follows plan cadence: Essential one-time guided; Plus quarterly; Complete monthly. Broker processing can take 7-45 days. Listings may return.

Free scan and instant results. The scan is free with no card required. Results appear when scanning completes; timing varies. A scan is not removal, paid monitoring or a complete cybersecurity assessment.

Money and insurance. Savings are individual, not guaranteed. Some cancellations require member action. Insurance is subject to policy terms, conditions and exclusions. Availability is U.S. only. Task Force is not a credit repair service.

Enterprise security thinking describes a layered approach, not an independent certification or a managed corporate security service.

TASKFORCE

STOP WONDERING.
SEE YOUR EXPOSURE.

Your information may already be out there.
Find out where. Decide what happens next.

1 ENTER YOUR DETAILS

Provide the details requested to match your records.

2 REVIEW YOUR RESULTS

See the personal information the scan finds exposed.

3 PUT PROTECTION TO WORK

Choose a plan to begin removal and activate protection.

RUN MY FREE EXPOSURE SCAN

INSTANT RESULTS. NO CREDIT CARD REQUIRED.

GETTASKFORCE.COM/SCAN

Results appear when the scan completes. Timing varies.
Removal and ongoing protection require a paid plan.