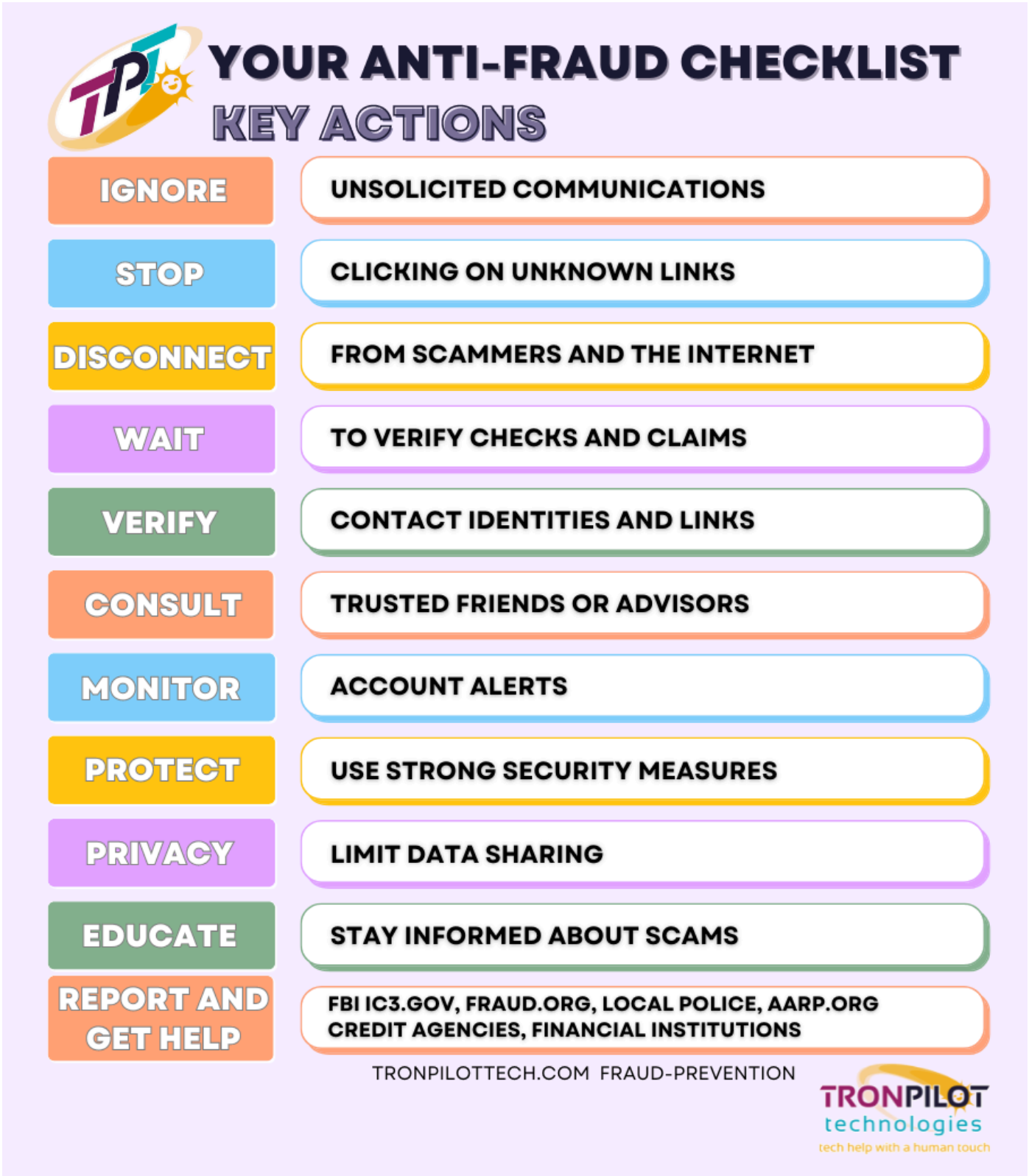
YOUR ANTI-FRAUD CHECKLIST
KEY ACTIONS
IGNORE
UNSOLICITED COMMUNICATIONS
STOP
CLICKING ON UNKNOWN LINKS
DISCONNECT
FROM SCAMMERS AND THE INTERNET
WAIT
TO VERIFY CHECKS AND CLAIMS
VERIFY
CONTACT IDENTITIES AND LINKS
CONSULT
TRUSTED FRIENDS OR ADVISORS
MONITOR
ACCOUNT ALERTS
PROTECT
USE STRONG SECURITY MEASURES
PRIVACY
LIMIT DATA SHARING
EDUCATE
STAY INFORMED ABOUT SCAMS
REPORT AND GET HELP
FBI IC3.GOV, FRAUD.ORG, LOCAL POLICE, AARP.ORG
CREDIT AGENCIES, FINANCIAL INSTITUTIONS
TRONPILOTTECH.COM FRAUD-PREVENTION
TRONPILOT technologies
tech help with a human touch

Your Anti-Fraud Checklist

🚫 Ignore:

- ☐ Ignore unsolicited calls, emails, texts, and social media messages.
- ☐ Respond only to known contacts. If unsure, always verify!

🛑 Stop:

- ☐ Do not click on pop-ups, links, or attachments from unknown sources.
- ☐ Do not contact numbers provided in unsolicited messages.
- ☐ Do not give control of your computer to unknown individuals.
- ☐ Do not share personal information over the phone unless you initiated the call to a verified number.

🔌 Disconnect:

- ☐ End communication with suspected scammers.
- ☐ Disconnect from the internet and shut down your device if you see suspicious pop-ups or locked screens.
- ☐ Avoid opening email attachments from unknown senders.

⏳ Wait:

- ☐ Resist pressure to act quickly; take your time to verify the situation.
- ☐ Wait for checks to clear before acting on them to avoid overpayment scams.

✔️ Verify:

- ☐ Independently verify the identity of contacts by looking up their official contact information.
- ☐ Only download apps and software from verified, trusted sources.

👥 Consult:

- ☐ Discuss unusual communications with trusted friends or advisors.
- ☐ Research online for reports of similar scams.

📈 Monitor:

- ☐ Set up alert notifications for transactions and changes in your online accounts.
- ☐ Verify alerts for any transactions you make.

🔒 Protect:

- ☐ Use strong, unique passwords for each account.
- ☐ Enable multi-factor authentication (MFA).
- ☐ Keep software and systems updated.
- ☐ Use secure Wi-Fi and ensure your home Wi-Fi has a strong password.
- ☐ Use reputable anti-virus software and firewalls.
- ☐ Enable pop-up blockers.
- ☐ Use a credit monitoring service and place credit freezes/locks.

🛡️ Privacy:

- ☐ Adjust privacy settings on devices and online accounts to limit data sharing.
- ☐ Properly dispose of personal documents.
- ☐ Be cautious about sharing personal information; use fake details for non-essential services.
- ☐ Pre-authorize who can access your personal health information.

📚 Educate:

- ☐ Stay informed about new scams by subscribing to newsletters from AARP, FTC, NCOA, CFPB, and Fraud.org.

Be Fraud-Free! Protecting Yourself from Modern Tech Scams

From Mark Annati's Fraud Prevention Presentation

Protective Steps Checklist

Strengthen Your Online Security

- ☐ **Use Strong, Unique Passwords**: Create long, complex passwords for every account. Avoid using easily guessed personal details (like birthdays or pet names).
- ☐ **Update Passwords Regularly**: Change passwords for sensitive accounts periodically.
- ☐ **Avoid Reusing Passwords**: Ensure each password is unique to prevent a data breach on one account from affecting others.
- ☐ **Utilize a Password Manager**: Use a password manager (e.g., Bitwarden, LastPass, Dashlane, etc.) to generate and securely store unique passwords.
- ☐ **Enable Multi-Factor Authentication (MFA)**: Add a second verification step to all your accounts. Using SMS or Email for codes is OK, but you can make it much more secure by using an authenticator app (like Google Authenticator, Microsoft Authenticator, etc.) or hardware security keys (like YubiKey) for greater security.
- ☐ **Consider Passkeys**: Use passkeys where supported. These are more secure than passwords, phishing-resistant, and utilize public-key cryptography.
- ☐ **Regularly Update Your Software**: Enable automatic updates on all devices to apply the latest security patches - for the operating system, and all the different applications on your device.
- ☐ **Enable Pop-Up Blockers**: Prevent malicious pop-ups with a browser-based blocker.
- ☐ **Manage Cookies:** Select "Manage Preferences" or "Settings" instead of "Accept All." Only allow essential cookies; reject tracking and marketing cookies.

Secure Wi-Fi and Internet Use

- ☐ **Turn Off Bluetooth, and/or Wi-FI:** If Not in active use, turn these services off.
- ☐ **Use a VPN**: Encrypt your traffic when using public Wi-Fi to prevent data interception.
- ☐ **Use a Secure Router**: Change the default admin password and use WPA3 encryption.
- ☐ **Avoid Public Wi-Fi for Sensitive Transactions**: Use your mobile data or a VPN (virtual private network).

Protect Your Cloud Accounts

- ☐ **Clean up unused devices:** Remove any old or unused devices connected to your cloud account.
- ☐ **Add recovery options:** Set up alternate email addresses and phone numbers for account recovery.
- ☐ **Use secure recovery methods:** Create and store recovery keys securely.
- ☐ **Update security questions:** Ensure answers to security questions are strong and not easily guessable.

Secure Your Devices

- ☐ **Use Antivirus and Anti-Malware Software**: Install reputable antivirus software and schedule regular scans.
- ☐ **Activate Device Encryption**: Turn on full-disk encryption (BitLocker for Windows, FileVault for Mac) to protect data if the device is lost or stolen.
- ☐ **Set Strong Device Locks, Passcodes**: Use strong PINs or biometric authentication like fingerprint or facial recognition to lock your devices.
- ☐ **Enable Recovery Options**: Set up alternate email addresses and phone numbers for account recovery. Ensure all account recovery options are current and secure.
- ☐ **Enable Auto-Backup Options**: Back up your phone or device's data to a secure cloud account regularly.

- [ ] **Review App Permissions**: Regularly audit app permissions and only grant necessary access (e.g., location, camera, contacts, etc.).
- [ ] **Disable Unused Features**: Turn off Bluetooth, NFC, and location tracking when not in use.
- [ ] **Enable Remote Wipe**: Use services like "Find My" to locate, lock, or erase data remotely if needed.
- [ ] **Prevent Phone # Port - Carrier PIN**: Set up a PIN with your carrier to prevent unauthorized SIM swaps.
- [ ] **Monitor Phone Account Changes**: Receive alerts for any modifications to your phone account.

Manage and Protect Your Personal Information

- [ ] **Be Cautious with Sharing Information**: Limit sharing personal data on social media and untrusted websites.
- [ ] **Adjust Privacy Settings**: Configure privacy settings on social media and online accounts to restrict data visibility.
- [ ] **Shred Sensitive Documents**: Use a shredder to destroy documents containing sensitive information before disposal.
- [ ] **Opt-Out of Prescreened Credit Offers**: Visit OptOutPrescreen.com to reduce mail theft risk.
- [ ] **Use Fake Details for Non-Essential Services**: Use pseudonyms or fake information for accounts that don't require real details.
- [ ] **Review Credit Reports Regularly**: Obtain free annual reports from Equifax, Experian, and TransUnion at AnnualCreditReport.com. Dispute any inaccuracies.
- [ ] **Place a Credit Freeze**: Freeze your credit with all major bureaus to prevent new accounts from being opened in your name.
    * **Equifax**: www.equifax.com | Phone: 1-800-525-6285
    * **Experian**: www.experian.com | Phone: 1-888-397-3742
    * **TransUnion**: www.transunion.com | Phone: 1-800-680-7289
- [ ] **Secure Your Snail Mail**: Use a locked mailbox or a PO box for sensitive mail.
- [ ] **Emergency Document Kit**: Keep photocopies of important documents in a secure, fireproof safe.

Secure Your Financial Accounts

- [ ] **Be Careful with the Cards:** Avoid using a Debit Card, and instead use a Credit Card. And better, use Apple Pay, Google Pay, or other secure payment apps instead of physical credit cards.
- [ ] **Set Up Account Activity Alerts**: Enable transaction alerts for all banking and credit accounts, as well as account logins and changes.
- [ ] **Use Virtual Credit Cards**: Consider using virtual cards for online purchases to protect your real credit card number.
- [ ] **Limit Debit Card Use**: Prefer credit cards for online transactions due to better fraud protections.
- [ ] **Secure Your IRS and Social Security Accounts**: Create accounts on the IRS and Social Security websites and secure them with MFA.
- [ ] **Regular Backups**: Keep offline backups (e.g., on an external hard drive) and cloud backups. Encrypt these backups for additional security.
- [ ] **Data Recovery Strategy**: Have a plan to recover from ransomware attacks or data loss.
- [ ] **Manage Checks and Financial Data:**
    - [ ] Use indelible ink when writing checks; never leave blank spaces.
    - [ ] Disguise checks when mailing them (e.g., inside a greeting card).
    - [ ] Write "For Deposit Only" on the back of checks to limit fraud risk.
    - [ ] Regularly review and balance your checkbook.

Lost or Stolen Phone Checklist

- [ ] **Activate 'Find My':** Use "Find My Device" to locate or lock your phone immediately.

- [ ] **Contact Your Cel Service:** Notify your carrier to block your number and prevent unauthorized use.
- [ ] **Change Passwords:** Change passwords for cloud accounts and financial apps linked to the phone.
- [ ] **Notify Important Institutions:** Inform financial institutions if banking apps are on the device.
- [ ] **Remote Wipe:** Consider erasing your phone's data remotely if you can't retrieve it.

Behavioral Security Practices

- [ ] **Ignore Unsolicited Communications**: Do not respond to unsolicited calls, emails, or texts. If unsure, independently verify using trusted contact information.
- [ ] **Avoid Clicking on Unknown Links**: Never click on links from unknown sources. Hover over links to see the actual URL and verify legitimacy.
- [ ] **Verify Senders:** Verify the sender's email address before responding.
- [ ] **Caution with Downloads:** Use only trusted sources for downloads and software.
- [ ] **Be Aware of Common Phishing Tactics**: Look out for urgency, threats, or too-good-to-be-true offers. Verify suspicious requests independently.
- [ ] **Stay Updated on Scams**: Follow newsletters from trusted sources like the FTC or AARP.
- [ ] **Contact Trusted Institutions**: Verify any suspicious requests using official contact details.
- [ ] **Know How Vulnerable You Are**:
    - [ ] **Have I Been Pwned**: Check for data breaches at haveibeenpwned.com.
    - [ ] **Firefox Monitor**: Check email breach history at monitor.firefox.com.
    - [ ] **CyberNews Personal Data Leak Checker**: Assess personal data exposure at cybernews.com/personal-data-leak-check.
- [ ] **Teach Children About Online Safety**: Use parental control software and discuss the risks of oversharing.
- [ ] **Help Elderly Family Members**: Assist in setting up and managing security settings.

Actions if You Believe You Are Being Defrauded

- [ ] **Stop Engaging with Scammers**: Disconnect immediately if you suspect fraud.
- [ ] **Shut Down Devices**: Disconnect from the internet to limit further access.
- [ ] **Check for Unauthorized Activity**: Review your credit reports and set up alert notifications.
- [ ] **Change Passwords**: Update passwords and enable MFA immediately.
- [ ] **Report Fraud**: Notify the appropriate authorities https://www.ic3.gov/ and financial institutions
- [ ] **File a Report with the FTC**: Use IdentityTheft.gov for a recovery plan.
- [ ] **Notify Financial Institutions**: Report fraudulent activity to your bank.
- [ ] **Contact Law Enforcement**: File a police report and report internet crime to IC3.gov.

Steps to Start Fresh and Protect Against Hackers

- [ ] **Obtain New Devices**: Purchase a new computer and a new phone with a different carrier.
- [ ] **Install Security Software**: Use antivirus and VPN software on the new computer to secure it immediately.
- [ ] **Set Up a New Email and MFA**: Create a new email account with strong security settings. Set up MFA using an authenticator app or hardware key.
- [ ] **Re-Secure All Online Accounts**:
    - [ ] Make a list of critical accounts and change passwords on the new, clean computer.
    - [ ] Use your new phone number and email for account recovery settings.
- [ ] **Prevent Cross-Contamination**: Do not use old, compromised devices to access new accounts. Only transfer data after scanning for malware. Avoid reinstalling potentially compromised files.
- [ ] **Avoid Clicking on Suspicious Links**: Be cautious and verify the sender before interacting with any link or attachment.