Secure NOC

Protect Your Privacy

Reduce Your Digital Footprint

Every account created, email sent, image posted, or location tagged adds to a person’s digital footprint. That information is combined to portray a digital image of someone's interests, hobbies, actions, beliefs, and routines. This information can be used by marketing companies to send targeted advertisements, but even worse it can be used by cybercriminals to commit identity theft.

Learn how you can keep your personal information protected by reducing your digital footprint!

- *Delete or Deactivate Old Shopping & Social Media Accounts*
  Though not in use, old shopping and social media accounts still contain your financial and personal information. Instead of risking a potential breach in one of those accounts, gain peace of mind by deleting or deactiving those accounts. For any account, app, or website that you no longer use or visit you should go to the account settings and look for an option to deactivate or close your account.
- *Deactivate Old Email Accounts*
  As email has evolved over the years most accounts become abandoned and sit idle. Emails house personal details about our lives, as well as sensitive information in old messages. When not in use, it can become difficult to notice if the email account has been breached. Instead of allowing them to pose a risk, delete them altogether.
- *Check Your Privacy Settings*
  Privacy and security settings change often. This is especially true on social networking sites such as Facebook and Instagram. Be sure that you are not sharing your private information with strangers. Periodically review your privacy settings and set them to your preference.
- *Disable Location Tracking*
  Location tracking allows you to get location-based suggestions on your searches for businesses in your area. Though convenient, it can pose a security risk if you allow your location to be tracked all of the time. Be sure you are aware of which apps and services have access to your location and that the location is only being tracked while using the service.
- *Think Before Posting*
  With dozens of social networking platforms available it is easy to share your thoughts, comments, and pictures with just about everyone. Be sure you are not oversharing your personal details on a social networking site. You should not post anything that you would not want your employer or your parents to see. Once something is posted on the Internet, it can be near impossible to have it removed.
- *Unsubscribe from Mailing Lists*
  Sometimes while browsing or shopping online we may sign up to be on a mailing list. Perhaps it is to receive the latest discounts and coupons. Over time those mailing lists add up and soon you are subscribed to hundreds of mailing lists. Most people don't read all of the newsletters and advertisements that clutter their inboxes. To reduce your digital footprint and the number of third parties with access to your information, start unsubscribing from the extra lists you don’t really need.

Social Media Privacy

Social networking sites can be a great way to share and connect with friends and family. However, users need to be mindful of the personal information that is being shared and the privacy risks associated with each of these accounts.

Outlined below are the steps that can take to help keep your most sensitive information safe on social media sites. Use these steps to help protect yourself and keep your information private.

Manage Accounts Securely

- *Configure your privacy settings to your preference*: Check the security and privacy settings in your social media apps and websites and enable/disable the privacy settings that you feel comfortable with. You can limit access to your account to only approved friends and enable restrictions on posts so that it is only visible to users of your discretion.
- *Manage third-party apps*: If you use your social media account to log in to other sites or allow apps to access and authorize your account, periodically review those application settings to ensure they aren't authorizing more than needed. Remove any applications that are no longer in use. Only allow trustworthy and secure third-party apps to your account.

Share With Care

- *Avoid sharing your location through geotagging*: Geotagging adds geographical identification data to posted photos, videos, websites, and messages through location-based applications and turns those posts public allowing anyone to view your content. Disable location services in apps or mobile devices when they aren't necessary.
- *Only friend or follow trustworthy individuals*: Don't accept friend or follow requests if you are unsure who the person is or if their account looks suspicious. Block or report suspicious accounts.
- *Don't overshare information*: Some things should not be posted or shared on social media. You do not need to add things like your full birthday, phone number, where you've lived in the past, and where you work on your social media profile.
- *Watch out for tagged posts*: Enable settings that allow you to review tagged posts before they are shared. Watch what you are tagged in and don't approve tags that share more than what you are comfortable with.
- *Beware of compromised accounts*: Be wary if you receive a suspicious message out of the blue from a friend or someone you follow. If the message contains a link do not click on it. Instead, contact the person directly through a trusted channel such as by phone and report the message.

Be Proactive

- *Protect yourself from harassment*: Learn about the options for blocking, muting, and reporting inappropriate behavior on the services you use.
- *Limit your profile visibility*: Use settings that prevent your profile from being publicly searched.
- *Block social media trackers*: Trackers are placed by social networks on other websites to follow what you do, see, and watch online. This allows social media companies to collect data about you in addition to what you already share on your profile. Install a secure browser extension that blocks trackers or use Content Blocking in Firefox.
- *Become familiar with the company privacy policy*: Social media networks periodically update their privacy policy. It is important to understand how the company is protecting your privacy.

Identity Theft Protection

Identity theft occurs when someone uses a combination of another person's personally identifiable information (PII) such as full name, birthdate, Social Security number, driver's license number, credit card number or other types of identifying information to take on that person's identity in order to commit fraud or other crimes.

5 Ways to Help Protect Your Identity
IdentityTheft.gov Helps You Report and Recover from Identity Theft
Visit the Federal Trade Commission's (FTC) Warning Signs of Identity Theft for more information.

If You Suspect Your Identity Has Been Compromised

Place a fraud alert on your credit report. A fraud alert can make it harder for an identity thief to open more accounts in your name.

Fraud alerts can be placed on your credit report prior to becoming a victim of identity theft, such as if you lost your Social Security card or other personal information. The alert lasts one year, but can be renewed. For victims of identity theft, an extended fraud alert will protect your credit for seven years. Learn how to place a fraud alert by visiting Federal Trade Commission's Identity Theft Information.

For more information on how to replace lost or stolen identification card visit the USA.gov Replace Your Vital Records webpage.

Consider putting a credit freeze on your account. Placing a credit freeze allows you to restrict access to your credit report making it difficult for identity thieves to open new accounts in your name. Most creditors look at your credit report before opening a new account. But if you've frozen your credit report, creditors can't access it, and probably won't approve fraudulent applications. You will need to ask for the credit freeze to be lifted before applying for new credit or doing business that may rely on someone checking your credit. You can place a freeze on your own credit files and on those of your children age 16 or younger. For more information refer to Federal Trade Commission: Credit Freeze FAQS.

Report identity theft to the federal government online or by phone. Visit the Federal Trade Commission's Identity Theft webpage to report identity theft and get a recovery plan. Create an account to update your recovery plan, track your progress, and receive prefilled form letters to send to creditors. This website provides additional resources and guides for identity theft victims. You can also call to file a report at 1-877-438-433 but you will not receive an ID theft report or recovery plan.

Complete the Internal Revenue Service (IRS) Identity Theft Affidavit, Form 14039. The form can be completed online on the FTC Identity Theft or you can download Form 14039 in PDF format for electronic filing.

Report the identity theft to the police. You should report the fraud to your local police station if you know the identity thief, the thief used your name in an interaction with the police, or a creditor or another company requires you to provide a police report. This will allow you to send a copy of the Identity Theft Report to creditors that require evidence that you allege a crime has occurred.

Report the identity theft to other organizations. Aside from reporting the fraud to one of the three major credit reporting agencies, you will want to contact your financial institution's fraud departments as well any retailers or companies where the thief opened an account.