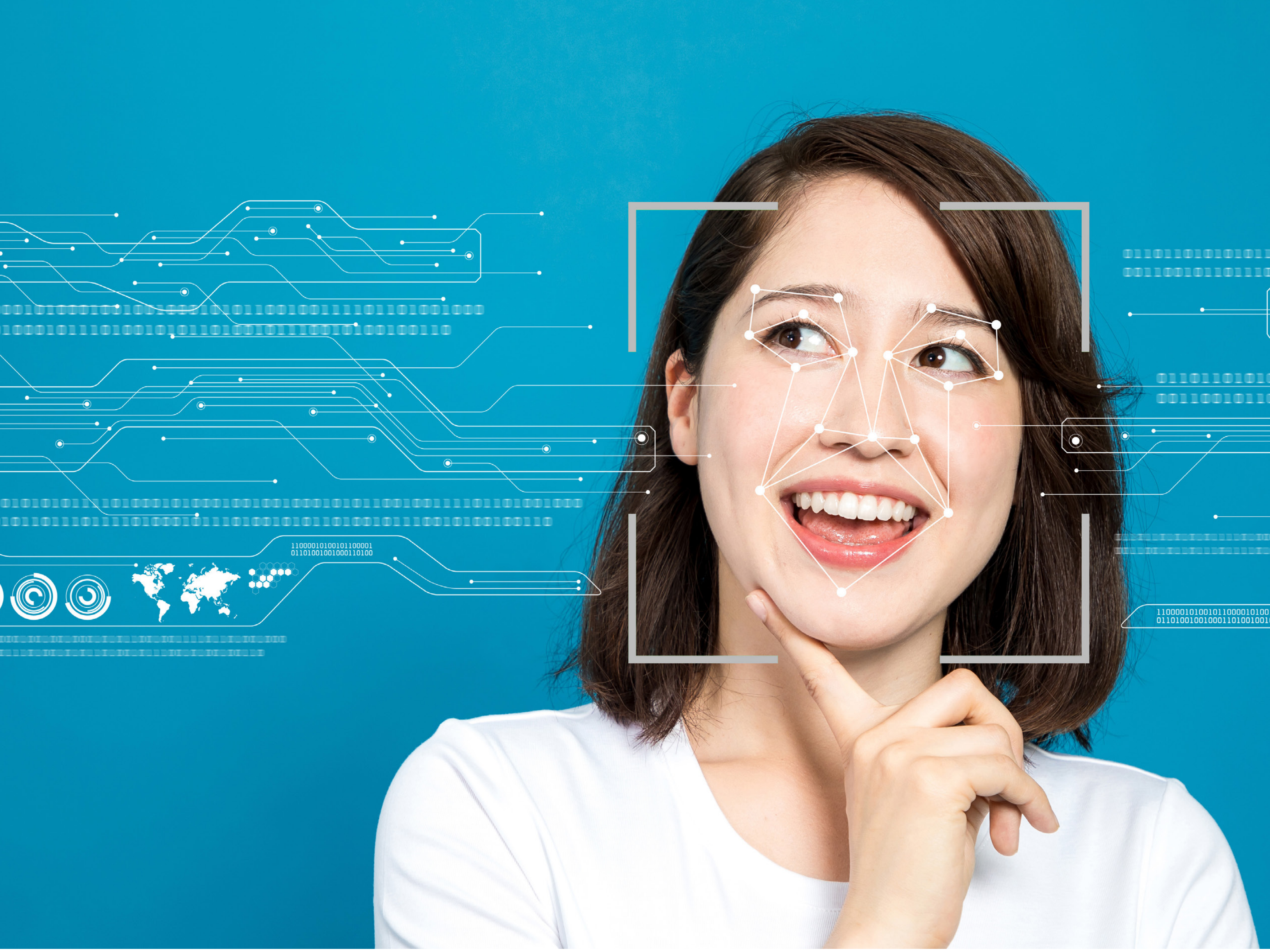


IDENTITY HYGIENE

Tips for Taking Care of Your Digital Self

Nationwide®

In partnership with
Generali Global Assistance and the
Identity Theft Resource Center

PRESIDENT & COO, GLOBAL IDENTITY PROTECTION SERVICES
GENERALI GLOBAL ASSISTANCE (GGA)
Paige L. Schaffer

PRESIDENT & CEO
IDENTITY THEFT RESOURCE CENTER (ITRC)
Eva Velasquez

CONTRIBUTORS
Nikki Fiorentino, ITRC
Kelly Dwyer, ITRC
Alex Hamilton, ITRC
Karen Barney, ITRC
David Brown, GGA
Megan Dwoskin, GGA
Laurel Laluk, GGA
Julie Yoo, GGA

CONTACT
Eugenia Buggs
VP, Global Marketing, Identity Protection Services
Generali Global Assistance
4330 East West Hwy Suite 1000
Bethesda, MD 20814
240-330-1091
eugenia.buggs@us.generaliglobalassistance.com

INTRODUCTION

Every day we follow little steps to take care of ourselves and make sure we stay healthy. We brush our teeth twice a day; go to the doctor for our annual check-up; see our hair stylist or barber regularly. We want to look and feel our best each day and for the long term. However, as our lives become more and more digital, we often ignore an important something that needs care as well: our identities.

The old saying "an ounce of prevention is a worth a pound of cure" is true for both our physical health and digital lives. We need to manage our identities just as we would other aspects of our physical, financial and emotional health. Identity hygiene refers to ongoing proactive maintenance that individuals, families and organizations take to ensure that their sensitive information remains as safe as possible. These habits are not only preventative, but take minimal amounts of time and are extremely effective when done regularly.

The first step in identity hygiene is understanding that identity theft and fraud are very real problems. In 2017 alone, there were 16.7 million victims of identity fraud in the United States. Since 2012, $112 billion, or $35,600 every minute, has been stolen as a result of identity fraud. Many Americans will become a victim of identity theft soon, if they haven't already. The effects of identity theft are not just financial in nature. Three-quarters of respondents in an Identity Theft Resource Center survey experienced severe distress over the misuse or attempted misuse of their personal information. In the following pages we've outlined ways to improve your identity hygiene and protect yourself from the long-term consequence of identity theft.

CONTENTS

April 2018

PASSWORDS

Passwords remain the most common form of protecting accounts of all kinds and are incredibly important in maintaining good identity hygiene. An online survey recently showed that the average person has 27 unique logins that require a password.   Possibly because we're inundated with passwords at every turn, nearly 70 percent of Americans have given up on trying to secure them. One study showed that 80 percent of Americans over the age 18 use the same passwords across multiple accounts and that people shared their passwords with 2-3 people on average. So what can you do to up your password game?

One result of bad passwords? In 2016, 63% of data breaches were linked to weak or stolen passwords.

ACTIONS YOU CAN TAKE

- **Change passwords every other month.** Make sure a password is at its best by changing it up. Set a reminder on your calendar or on your phone's alarm. If your password is hacked, it will only be useful to crooks for a couple months at most.

- **Use good passwords.** Create strong passwords with numbers, symbols, and uppercase and lowercase letters. Long, memorable phrases may be even better.

Bad Password	Good Password
password	*My2ChihuahuasareRunning!*

- **Use different passwords.** Make sure to use different passwords on each account so that if one account is compromised it doesn't mean they all are.

- **Consider using multi-factor authentication.** This is a system that uses two different avenues to verify who you are. For example, a login password and a code that's texted to your mobile phone.

TOOLS AND RESOURCES

- **Password Generator:** Online services like random.org can help develop passwords of any length and complexity.

- **Password Manager:** Can't remember a password? With many password managers, you only need to remember is a key password and the manager does the rest.

CREDIT REPORTS

Annual check-ups at the doctor can help catch minor health problems before they become major afflictions. Just as a doctor helps you understand what's going on inside your body, a credit report lets you see what's going on with part of your identity. Credit reports are issued by three major credit bureaus in the United States and provide a snapshot of your financial history. They're often used by lenders, utility companies, employers, or landlords when they're assessing your financial stability because they include where you've lived, bill payment history, amount of money you've borrowed, and how much you've paid back.

Checking your credit report regularly helps to ensure that someone else isn't using your name to open credit cards, apply for loans, or start new utility services and leaving you to foot the bill. Fraud that impacts your credit report can decimate your credit and good standing, making future financial decisions even more complicated and costly.

It isn't just banks that look at credit reports. Jobs which require a background check can be lost due to erroneous reporting on a credit report due to identity theft.

ACTIONS YOU CAN TAKE

- **Check credit reports at least three times a year.** This frequency helps you keep an eye on anything new or erroneous that and can alert you to take action if needed.
- **Look for red flags.** Any information that is inaccurate on a credit report may be a sign of identity theft. You can contact the credit bureau and report false information.
- **Consider placing fraud alerts.** Each bureau allows you to set up an alert that will require lenders to inform you if they access your credit report. This can serve as a "double check" and could reduce the risk of fraudulent activity.

TOOLS AND RESOURCES

- **Free Credit Reports:** You can obtain a credit report for free from each of the three credit reporting agencies every year at www.annualcreditreport.com.
- **Credit Monitoring Services:** Many identity protection programs can simplify your credit protection strategies by providing regular access to your credit reports and scores, notifying you in case of suspicious activity, and working with the credit bureaus to place alerts and correct errors.
- **Nerdwallet's Guide to Reading Your Credit Report:** Helpful tips and information on how to read and understand a credit report.

ACCOUNT STATEMENTS

More than 40 percent of Americans have experienced fraudulent credit card charges. With the increase of online shopping and banking, fraudulent card use shifted in 2016 from stolen or counterfeit cards being used in-person to the account numbers being used remotely. This means it is more important than ever to regularly check statements. While your card may be in your wallet, that doesn't mean it isn't being used by a criminal somewhere.

But it's not just your financial accounts that are targeted by identity thieves. Health insurance statement of benefits may alert someone that their identity was used to obtain medical services or prescriptions, known as medical identity theft.

Take a minute to look at the bank's policies and understand what they mean. Most financial institutions will give you 30 days to report fraudulent charges before having to de-facto accept them.

ACTIONS YOU CAN TAKE

- **Check statements often.** Don't go too long without reporting a fraudulent charge, or there may not be a way to get the money back. *Read credit card statement carefully.* Sometimes thieves use small purchases to see if the card will work for larger purchases.

- **Review all account statements - even loyalty accounts and medical service statements.** Look at these just as carefully as financial statements as they can indicate medical identity theft or other problems.

- **Inform the company at the first sign of suspicious activity.** Consumers may only have a limited amount of time to report suspicious activity before it can no longer be disputed.

- **Consider a paid identity monitoring service.** Companies use a combination of technology and human intelligence to search the deep and dark web where stolen data is bought and sold. They can help alert you if your personal information is compromised and assist in taking steps to further protect you.

TOOLS AND RESOURCES

- Tips to Prevent Medical Identity Fraud from the Medical Identity Fraud Alliance

RECORDS AND DOCUMENTS

More than 40 percent of Americans have experienced fraudulent credit card charges. With the increase of online shopping and banking, fraudulent card use shifted in 2016 from stolen or counterfeit cards being used in-person to the account numbers being used remotely. This means it is more important than ever to regularly check statements. While your card may be in your wallet, that doesn't mean it isn't being used by a criminal somewhere.

But it's not just your financial accounts that are targeted by identity thieves. Health insurance statement of benefits may alert someone that their identity was used to obtain medical services or prescriptions, known as medical identity theft.

Believe it or not, dumpster diving is still a method identity thieves use to get personal information.

ACTIONS YOU CAN TAKE

- **Shred documents once a week.** Shredding documents is a really easy task that can pay off in the long run. You don't have to shred everything, but anything with sensitive personal information should be shredded using a cross cut shredder. Pay special attention to credit card offers.
- **Ensure proper storage of sensitive documents.** Make sure to do this right away after using them.
- **Make sure that electronic copies are completely destroyed when no longer needed.** Remember, even sending documents to a computer's recycle bin isn't enough. Empty it after putting something in there. Otherwise, it is accessible to anyone who is able to get on that computer.
- **Go through email once a month to ensure that no sensitive information or documents are there.** Find some? Delete or properly store them.
- **Go through purses or wallets once a month to make sure that they don't contain any sensitive personal information that's not needed.** Don't regularly use that checkbook? Take it out and store it somewhere safe.

TOOLS AND RESOURCES

- **Wallet List:** Make a list of all of the cards and documents kept in a wallet or purse with the phone numbers to call if they are lost a stolen. Make sure to store it someplace safe.
- **Free Shredding:** Often times there are community events where people can go to shred documents if they do not have an at-home shredder. Make sure to do the shredding or monitor the attendant as they do it.

SOCIAL MEDIA

Social media is rife with identity threats, such as scams, oversharing and reputation damage. In order to practice good identity hygiene, constantly be aware of what is being shared and what kind of information those posts and pictures give away to strangers. When online, be critical of messages and posts that may lead to becoming a victim of a scam. Messages from “friends” claiming they are in trouble and need money, or deals that seem too good to be true, can lead to having an identity stolen or being scammed out of hard-earned money.

Social media platforms may not alert users when they change their privacy settings, meaning that what a user thought was once private and only available to friends could easily become viewable to anyone.

ACTIONS YOU CAN TAKE

- **Check social media platforms for updates to the privacy settings once a month.** A user may not be notified if the settings change, so don’t want to be left unaware.

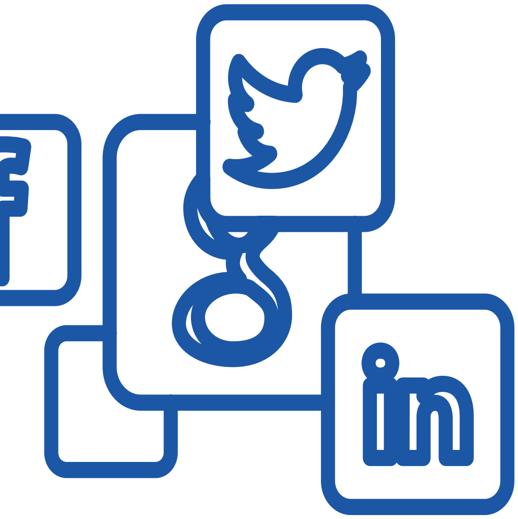
- **Think about any image or statement posted online before it’s posted.** Whether things are set to private or not, think about the repercussions if someone saw then that shouldn’t.

TOOLS AND RESOURCES

- **Facebook’s Privacy Settings**: A one-stop shop for learning how to manage privacy settings on Facebook.

- **Twitter’s Guide to Safety:** Shows users everything from how to protect tweets to how to deal with a hacked account.

- **Instagram’s Privacy and Safety Center:** All about how to make sure an Instagram only shows what a user wants



CYBERSECURITY

Computers are a huge part of everyday lives and a personal information stored on them is a goldmine to identity thieves. Threats like ransomware (which literally holds a computer hostage until it's paid) or WiFi hacking can cause serious damage to someone's identity. Your technology is a gateway to your identity, and keeping them secure is more important than ever.

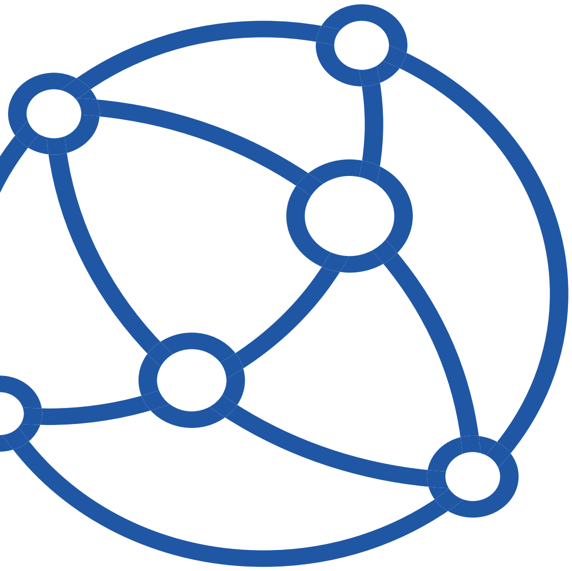
> In 2016, individuals were attacked by ransomware every 10 seconds.

ACTIONS YOU CAN TAKE

- **Make sure anti-virus and malware software is installed and up-to-date.** Install new updates as soon as they become available and check for new updates that may have been missed once a week.
- **Back up data.** One of the best ways to protect from the fallout of a ransomware attack is to back-up data externally each day. Data can be set to automatically back-up to the cloud through a subscription service or can be done manually for free to an external hard drive. That way, if hit by a ransomware attack, a user can just use their backup to regain access to their files.
- **Change the WiFi password once a month.** This will keep hackers (and neighbors) off of the connection and out of files.

TOOLS AND RESOURCES

- **National Cyber Security Alliance:** NCSA has tons of information and resources on how to keep safe online.



MOBILE DEVICES

The average American spends five hours a day on their smartphone.   Imagine all of the information stored on these little devices that never leave our side. Since a phone is basically a little computer, users should also take all of the same identity hygiene tasks used for good cybersecurity and apply them to their mobile devices. However, for the most part, good identity hygiene tasks are a one-time step each time consumers get a new device. Think of it as getting an annual booster shot or an immunization before traveling abroad. A new trip means new immunizations, and a new device means a new passcode, backup and tracking.

Even though it is one of the best ways to easily protect all the data on a mobile device, 28 percent of Americans do not use a screen lock on their mobile devices.

ACTIONS YOU CAN TAKE

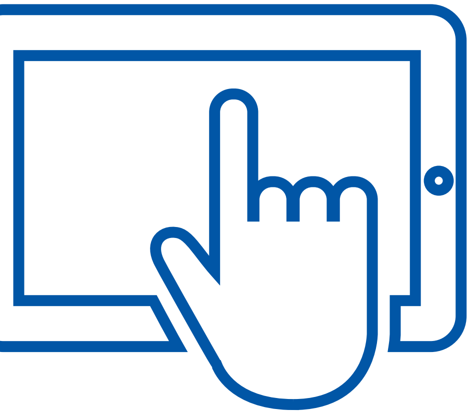
- **Use a Passcode.** The most important thing you can do to protect the information on your smartphone is to put a passcode on it, which only has to be done once.

- **Install a back-up and wiping app.** This will ensure that if a device ever becomes lost or stolen, the owner can erase all of the personal information on it without having physical access to the phone. The owner will also have all of the data ready to download to a new phone, making the decision to pull the plug on the missing device that much easier. Many of the backup and wiping programs also have a tracking feature to help find a phone, which can help if it's simply misplaced.

TOOLS AND RESOURCES

- **Find my iPhone:** This is the app developed by Apple itself to help locate an iPhone if it is lost or stolen.

- **Find my Mobile from Samsung:** This services can help find a Samsung phone if it is lost or stolen.



SPREADING GOOD IDENTITY HYGIENE

Now that you know all about creating and maintaining good identity hygiene, it is important to share that knowledge with those around you. This will help family, friends and co-workers, but it will also reinforce good identity protection habits. Share this information and lead by example at home, since children need to understand both the value of their personal information and the risks of not properly caring for it, just as you would teach them about their health. Likewise, greater numbers of senior citizens are enjoying online activity, so elderly parents need guidance as well. Continual practice of good identity hygiene will ensure that protecting one's identity will become as natural as brushing teeth or showering.

SUMMARY REFERENCES

Federal Reserve System. “Federal Reserve Payments Study (FRPS) 2017”. December 2017.

IBM Security. ”Future of Identity Study Consumer perspectives on authentication: Moving beyond the password”. January 2018.

Identity Theft Resource Center. Identity Theft: The Aftermath 2017. October 2 2017.

Ivanov, Antone and David Emm, Fedor Sinitsyn, Santiago Pontiroli. “Kaspersky Security Bulletin 2016. The ransomware revolution”. December 8 2016.

Javelin Strategy & Research” Identity Fraud Hits All Time High With 16.7 Million U.S. Victims in 2017, According to New Javelin Strategy & Research Study”. February 6 2018.

Keeper Security. “2017 Consumer Mobile Security App Use”. https://keepersecurity.com/assets/pdf/Keeper-Mobile-Survey-Infographic.pdf

Mitchell, Travis. “Password Management and Mobile Security.” Pew Research Center: Internet, Science & Tech, Pew Research Center, 25 Jan. 2017, www.pewinternet.org/2017/01/26/2-password-management-and-mobile-security/.

Olmstead, Kenneth, and Aaron Smith. “Americans and Cybersecurity.” Pew Research Center: Internet, Science & Tech, Pew Research Center, 25 Jan. 2017, www.pewinternet.org/2017/01/26/americans-and-cybersecurity/.

Simon, Khalaf. “U.S. Consumers Time-Spent on Mobile Crosses 5 Hours a Day.” Flurry Analytics, 2 Mar. 2017, flurrymobile.tumblr.com/post/157921590345/us-consumers-time-spent-on-mobile-crosses-5.

Verizon Enterprise. “2016 Data Breach Investigations Report”. April 2016. http://www.verizonenterprise.com/resources/reports/rp_dbir-2016-executive-summary_xg_en.pdf

Generali Global Assistance (GGA), proudly owned by Europ Assitsance Holding, a division of the multinational Generali Group, has been busy protecting clients and their customers for over 30 years–via co-branded services and behind the scenes as a client-branded provider. GGA was one of the first companies to provide identity theft resolution services in the United States. They are the identity protection engine behind some of the biggest names in the Fortune 500, and today are a leading provider, proudly protecting millions of lives from the growing threat of identity theft. Their comprehensive identity protection is a powerful combination of credit monitoring and alerts, advanced identity monitoring technology, online data protectoin tools, and award-winning resolution.

For more information about preventing identity theft for your employees, customers, or members, contact Generali Global Assistance Identity Protection Services at

GeneraliGlobalAssistance-IDP.com

GENERALI
GLOBAL ASSISTANCE

Founded in 1999, the Identity Theft Resource Center® (ITRC) is a nationally recognized non-profit organization established to support victims of identity theft in resolving their cases, and to broaden public education and awareness in the understanding of identity theft, data breaches, cybersecurity, scams/fraud, and privacy issues.

The ITRC provides no cost victim assistance and consumer education through its call center, website, social media channels, live chat feature and ID Theft Help Mobile App.

www.idtheftcenter.org

ITRC | IDENTITY THEFT
RESOURCE CENTER