



Landlords Helping Landlords

## CDARPO NEWSLETTER

September 2022

### What is it...or better – WHAT HAPPENED?



*Real World Problem: For the forensically-minded sleuths in our readership, can you piece together what happened in this scene...and what caused it? (Answers provided later in the newsletter.)*

Page 2 September Membership Meeting	Page 3 President's Message	Page 5 Advice to the Houselorn	Page 6 Volunteers & Coalitions  Page 7 Membership & Your Officers	Page 8 Forensic Follow-up: Answers to "Real World" Problem	Page 9 This Just In → HUD FMR Data	Page 10 Our Sponsors  Page 11 Attachment on Cybercrime Safety
--	----------------------------------	---	---	--	--	--

## **September 2022 Membership Meeting**

### **Topic: Panel Discussion on Landlord Experience**

Date: Thursday September 8, 2022 7:00 PM Eastern Time

**Location: In Person at the Courtyard by Marriott on River Street, Troy, NY**

or by Zoom at:

<https://us06web.zoom.us/j/84533058919?pwd=Y0hGNzllc3N3bVJ0UXNYaDlOdM5QQT09>

Meeting ID: 867 7663 8324      Passcode: 615092

### **Guest Speakers**

**Sean Daley**

**Mac Mowbray**

**Tom Vador**

Fellow Board members Sean, Mac, and Tom will lead an interactive panel discussion about their respective landlord experiences focusing mainly on the positive aspects of becoming a landlord. This will be an unscripted, open and informal educational opportunity to engage with experienced landlords and learn more about the how's and why's of being a landlord. Please bring your questions, and be prepared to engage with the panel – and even share your experiences.

CDARPO = Capital District Association of Rental Property Owners, Inc.

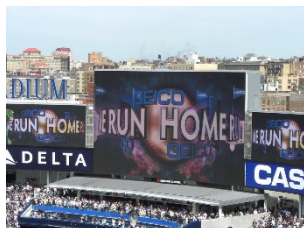
MAILING ADDRESS: CDARPO, PO Box 8, Latham, NY 12110

# PRESIDENT'S MESSAGE

Dear CDARPO Members:

Welcome to your September 2022 CDARPO Newsletter issue. While the membership was on a 2-month recess from regular meetings, the board remained busy orchestrating a successful summer outing and planning for CDARPO's future. In my comments this month I will recap the summer outing, welcome a new addition to our Board of Directors, and offer some timely information on protecting oneself from cybercrime.

## Summer Outing Success



CDARPO strives to have a summer event every year during our two-month recess from our regular monthly program activity.

Thank you to everyone who volunteered to organize our summer outing with the Tri-City ValleyCats. Our members enjoyed a fun evening of baseball, food, fireworks, and networking during our July evening event. A special shout-out to Karen and Eric Wentz! They hit a home run organizing and arranging the outing in the reserved suite looking out over home plate!

Thanks to all who joined us for the evening! A fun time was had by all! ... and our home team ValleyCats won!



## Board Of Directors Update

Please welcome Bryson Gibson as new "at-large" member of your Board of Directors. With your Board's approval Bryson fills a vacancy left by our departing Vice President. Bryson and his wife Caroline, have graciously volunteered to support your organization by taking on the challenge of improving and managing our social media presence. This help is very much needed to broaden CDARPO's reach and to stay relevant in a world that communicates in real-time (by photos, sound-bites, etc.). Additionally, a good social media presence will help attract and retain additional membership. Technology and demographics continue to evolve, and having a good social media strategy is imperative for your organization's evolution and longevity.

We currently have a modest Facebook presence; we're going to improve upon that!

We also are going to expand online to Instagram, Twitter and Nextdoor, and link these resources to our website.



## Preventing Identity Theft


Recently I was given some timely information regarding the topic of identity theft and how to prevent it. Here are some useful takeaways from information presented by retired FBI Agent Jeff Lanza, an expert on cybercrime.

- Everyone knows that there are three credit reporting agencies – Experian, TransUnion, and Equifax. Did you know there is actually a fourth? **Yes, it's called Innovis.** One of the best ways to prevent account fraud is to freeze all four credit reports. Restricting access to your credit reports is a proven way to prevent new account activity in your name. Remember, though; if you want to apply for a loan or new credit card, you would have to lift the freeze until you've secured those new instruments or loans.
- When writing checks, use a **gel pen!** Gel pen ink is much more difficult to "wash" than conventional pen ink. Who knew?!?
- For online account security, use **passphrases** instead of passwords. A passphrase is composed of a combination of words strung together that are familiar to you. You can relate your passphrase to your accounts – this means different passphrases for different accounts! Also take advantage of biometric security options offered by many online companies. These strategies protect against brute force attacks where hackers use powerful and sophisticated computer programs and algorithms to guess passwords. Passphrases also protect against "credential stuffing" where a hacker obtains a password for one site and uses it to hack another site.

See the sobering table below to understand

just how long it takes in 2022 to crack a password today based on its length and complexity.

TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2022					
Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	2 secs	7 secs	31 secs
8	Instantly	Instantly	2 mins	7 mins	39 mins
9	Instantly	10 secs	1 hour	7 hours	2 days
10	Instantly	4 mins	3 days	3 weeks	5 months
11	Instantly	2 hours	5 months	3 years	34 years
12	2 secs	2 days	24 years	200 years	3k years
13	19 secs	2 months	1k years	12k years	202k years
14	3 mins	4 years	64k years	750k years	16m years
15	32 mins	100 years	3m years	46m years	1bn years
16	5 hours	3k years	173m years	3bn years	92bn years
17	2 days	69k years	9bn years	179bn years	7tn years
18	3 weeks	2m years	467bn years	11tn years	438tn years

 > Learn about our methodology at [hivesystems.io/password](https://hivesystems.io/password)

Source: Hive Systems

You will find an attachment at the end of this newsletter; a comprehensive 5-page reprint entitled *"Simple Safeguards: How to Stay safe From Identity theft and Cybercrime"*. Mr. Lanza gave us his permission to reprint and distribute the reprint. Use this resource to protect yourself and your family from cybercrime.

Best regards,  
Tom Vador

President,  
Capital District Association of Rental  
Property Owners, Inc.

# ADVICE TO THE HOUSELORN

BY MAC MOWBRAY

A lookback into the CDARPO archives! The following was published in our September 2016 Newsletter...

Alas!! Fall is knocking at our doors! Now is the time to take a nice pre-fall day and do all the necessary chores that you ALWAYS put off until the last minute. I know I always harp and nag about this every year, but if I don't, I will get the calls asking what to do about that frozen drain pipe that is clogged up with (you guessed it) leaves, which you forgot to clean out in late September. Check the roof completely. That means not just the leaves and branches from summer windstorms, but moss, mildew and other foreign objects that may get thrown up by kids or dropped by birds. One caller was VERY distressed to find a medium sized rodent clogging her roof drain! Soda bottles, tennis balls and sneakers seem to find their way to the roof also. Unless you plan on watering in the fall, turn off outdoor faucets and drain and hang up hoses. (*ed. – Do not leave hoses connected to outdoor spigots during the winter.*) Next you will want to inspect all the vents, including dryer vents, chimneys, and exhaust fans. All of these things can cause fires or in some cases carbon monoxide poisoning. That of course leads to checking the carbon monoxide detectors and smoke alarms. Now is a good time to replace the kitchen smoke detector with ones that feature a "HUSH" button. That provides for a safer household. The reason being, when a tenant is cooking, they may remove the battery to stop the noise and often forget to replace the battery. With the hush button, they just touch the button when they are done cooking and the detector is back in operation. Schedule a cleaning and tune up of your heating equipment, especially if it is oil or kerosene fired. Natural gas needs less attention. Check your fire extinguishers if you have them. Ditto for the sprinkler system. Make sure your tenants have not blocked the fire escapes with plants, BBQ's or chairs. Remind them it is a fire escape and not a balcony! If you have yards or driveways, check and fill cracks. They will get bigger over the winter. Water gets in, freezes and forces the crack to open wider. All

basement windows and vents should be closed. Anything that could be damaged by snow and ice should be put away. You get the idea: check everything now, so that when winter is here you will not be stuck doing things in the freezing cold.

**"Latham" has a question about hoses:** I have several washers in my basement for tenant use. I noticed that a couple of the hoses seem to have bulges in them. They do not seem to be leaking. Is it something I should be worried about?

**Mac says:** Run - do not walk, do not pass go, do not collect \$200.00 - to the hardware or big box store and get enough BRAIDED STAINLESS-STEEL hoses to replace ALL of the hoses, HOT and COLD! In fact, before you do that, turn OFF the water to the bulging hoses ASAP. An unnoticed broken hose can put a lot of water in the wrong places in a very short time. Make sure all the new hoses have new washers in them. Never install a new hose using old washers, no matter how good they look. You did not ask this, but if you have to replace any of your washers, consider coin-operated ones. I have the honor system and it does not work very well. My next washer will be the coin operated model.

**"Downtown Troy" complains** some of the windows and doors are sticking. She asks: do I need to have them planed down? It will mess up the paint.

**Mac says:** Not necessarily. Take a bar of soap – Ivory is good – and rub on the surfaces that stick. When the humid weather is over, you can just wash the soap off the doors. Usually by the end of September this problem will take care of itself.

**Stains are bothering a "Delmar landlady".** She says: I have just had the apartments painted and after a couple of weeks some rusty looking stains appeared. Nothing is leaking up above and there were no stains there before. What's up with that? Is it the painter's fault?

**Mac says:** No, not if there were no visible stains there when they did the job. If there were, they would have taken care of it. Just get a can of alcohol base white paint (brand name BIN) by the Zinsser Company. Take a small brush, cover the stain and wait the suggested time and then touch up with the ceiling paint. Don't feel bad, it happened to me.

See you next month. -- Mac Mowbray

# VOLUNTEERS

CDARPO has no paid employees. **We operate entirely by volunteers** who unselfishly contribute their precious time to make your organization run as smoothly as possible with lots of meaningful content. CDARPO needs volunteers who are interested in serving in various capacities such as on the following committees:

- Membership
- Legislative Update
- Newsletter
- Speakers / Events

If this is something that interests you, please contact the board at [cdarpo@gmail.com](mailto:cdarpo@gmail.com) or Tom Vandor at [president@cdarpo.org](mailto:president@cdarpo.org).

# STAY CONNECTED

Current members should join our forum discussion area on Google groups. This is an email-based forum for exchanging ideas and interacting with fellow landlords that may have experiences to share. Send an email requesting access to:

[cdarpo-talk+subscribe@googlegroups.com](mailto:cdarpo-talk+subscribe@googlegroups.com)

or contact Marshall Miller at

<mailto:marshall@bluehattery.com> for more assistance.

Find us online at [CDARPO.org](http://CDARPO.org) and on [Facebook](https://www.facebook.com/cdarpo). Sign up for our newsletter on the [contact page](#) of our website.

Stay tuned for new and improved social media opportunities to stay connected and informed!

# COALITIONS

**CDARPO is a member of Under One Roof**, a coalition of landlords and landlord organizations, formed to represent landlord interests with issues arising from legislation passed and proposed in favor of tenant interests. Learn more at <https://www.underoneroofny.org>.

Based on recently enacted and newly proposed laws, private property ownership and the rights of private property owners in New York appear to be in serious jeopardy. To strengthen the voice of the small property owner CDARPO needs to partner with other like-minded associations around the state. If you have ideas on how to assemble a “meeting of the minds” please let us know. We’d like to create a strong coalition of landlord associations (and small business organizations) to improve our voice so that our local and state representatives hear our concerns and better act on our behalf.

**If you have ideas for content that you’d like to see covered in our monthly newsletter, please contact us. We will consider your idea and even give you an opportunity to author your own article!**

# MEMBERSHIP

Regular membership dues are \$75/year and include a 10-issue monthly newsletter, a members-only forum, a landlord help line, free advertising at meetings & more.

**Send membership inquiries to:** [membership@cdarpo.org](mailto:membership@cdarpo.org)

Commercial Membership dues will vary based on desired advertisement formats - please visit our [website](#) for more details.

## Meet Your 2022 Officers and Board Members

### Officers

**President:** Tom Vandor - [president@cdarpo.org](mailto:president@cdarpo.org)

**Vice President:** vacant

**Treasurer:** Sean Daley - [treasurer@cdarpo.org](mailto:treasurer@cdarpo.org)

**Secretary:** Lisa Benware - [secretary@cdarpo.org](mailto:secretary@cdarpo.org)

### Board Members:

Bryson Gibson - Mac Mowbray - Roland Nzaou - Eric Wentz - Karen Wentz

### Communications Liaison

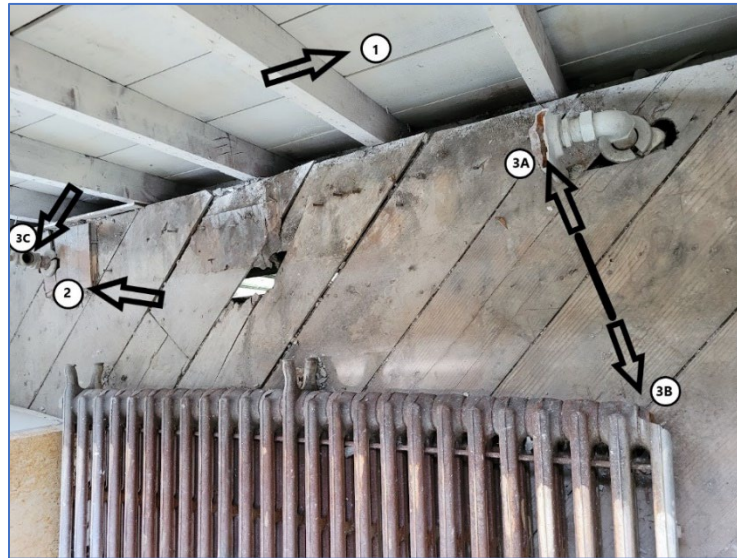
For inquiries, please contact Terrance Wansley - [communication@cdarpo.org](mailto:communication@cdarpo.org) or (518) 433-7377

---

*CDARPO does not give legal, tax, economic, or financial advice and disclaims all liability for actions resulting from communications with officers or members. Opinions contained within this newsletter are not necessarily those of the organization. Individuals are encouraged to consult legal or financial advisors for professional advice regarding such matters.*

---

Answers to the “Real-World” problem captured in the photo on Page 1:



So, what’s going on in this photo? What you see here is a 300-pound (+/-) cast iron hydronic radiator on its side laying on a subfloor in a residential kitchen the City of Albany. The radiator had burst during a freeze sometime during the winter of 2021-2022. Arrow #1 points to exterior wooden wall sheathing and wall studs that, strangely, appear to be painted white. That’s not just paint! It’s an EPA-certified mold encapsulant primer. It was applied after extensive demolition and dry-out of the moldy interior living spaces following a complete and extensive soaking while the burst plumbing and heating systems gushed water all over the premises for days.

Arrow #2 points to a very small patch of remnant original tongue-and-groove oak hardwood flooring that was laid down by craftsmen throughout the first floor of this residence about 100 years ago. Arrows 3A, 3B, and 3C point to where the cast iron failed, cracked and broke apart due to the immense forces caused by ice expanding inside the radiator while the water in the system froze due to lack of electricity and no boiler operation. At 3A there still remains a piece of radiator attached to the water supply pipe. Eleven additional radiators in this property suffered the same fate, and as you might imagine, caused a flood of problems affecting every element of the house system: plumbing, heating, electrical, rough and finish carpentry, foundation and structure, and contents.

Why is all of this relevant in a landlord association newsletter? Because, the root cause of the damage in this property was a bad decision by an experienced landlord to rent property to what turned out to be a thoroughly unqualified tenant... that vacated the property without notice and likely left a huge utility bill unpaid, which then prompted the utility company to terminate power in the middle of winter while city water pressure was still energizing the plumbing and heating systems. The state-imposed eviction moratorium exacerbated the problem to generate over \$125,000 in damage to what was a quaint house in a quiet neighborhood. Yes, negligence by the tenant really caused all the damage, but if that tenant never had possession in the first place, well then you likely know the rest...If you wish to learn more about how to minimize the risk of this type of problem, stay connected with CDARPO, and learn as much as you can from those of us who’ve weathered the storm – so to speak. Lessons abound in all of our members’ collective experiences. There still may be long-term opportunities in the rental marketplace. What will be required is a quantum shift in how “small” property owners manage the care and feeding of their hard-earned investments.

...to be continued.



## This Just In...

On September 1<sup>st</sup> the U.S. Department of Housing and Urban Development (HUD) published the Fiscal Year 2023 Fair Market Rents (FMR).

FMRs, published annually, are an estimate of the amount of money that would cover gross rents (rent and utility expenses) on 40 percent of the rental housing units in an area. Nationally, Per HUD, *"FMRs will increase by an average of approximately 10 percent, enabling more households with housing vouchers to access affordable, stable housing. For FY23, HUD is using private sector data to estimate changes in FMRs to address a temporary data availability challenge and to align with market conditions."*

The data at right reflect FMRs for the Capital District, which roughly corresponds to HUD's Albany-Schenectady-Troy, Metropolitan Statistical Area (MSA). The Albany-Schenectady-Troy, NY MSA consists of the following counties: Albany County, NY; Rensselaer County, NY; Saratoga County, NY; Schenectady County, NY; and Schoharie County, NY.

FMRs for MSAs nationwide are readily available at

<https://www.huduser.gov/portal/datasets/fmr.html#2023>.

Data are available at the MSA level **AND** by zip code, which will enable you to drill down with more granularity for your particular region of interest.

## Albany-Schenectady-Troy MSA FMRs

The FY 2023 FMRs are provided in the table below with comparisons to the FY 2022 FMRs. How do your rents compare?

**Final FY 2023 & Final FY 2022 FMRs By Unit Bedrooms**

FY	Efficiency	One-Bedroom	Two-Bedroom	Three-Bedroom	Four-Bedroom
2023	\$968	\$1,079	\$1,313	\$1,598	\$1,764
2022	\$890	\$991	\$1,207	\$1,492	\$1,637

Source: HUD

Investors already know that location matters. General averages for an area as large as the Capital District are interesting, but won't reflect differences within the sub-markets. Small Area Fair Market Rents (SAFMRs) are FMRs calculated for ZIP Codes within Metropolitan Areas. There are 151 zip codes within the Albany-Schenectady-Troy, NY MSA. The maximum, minimum, and median FMRs among the zip codes that comprise the Albany-Schenectady-Troy MSA are provided in the table below. Median values are not average values; they are middle values in a sorted list of values. So, half the rents are higher than the median, and half the rents are lower than the median. The final MSA FMR's will be closer to the average than the median.

**Max, Median, and Min FY 2023 SAFMRs in the Capital District**

	Efficiency	One-Bedroom	Two-Bedroom	Three-Bedroom	Four-Bedroom
Max	\$1,390	\$1,550	\$1,890	\$2,300	\$2,540
Median	\$920	\$1,020	\$1,240	\$1,510	\$1,670
Min	\$810	\$900	\$1,090	\$1,350	\$1,480

Source: HUD Small Area Fair Market Rents

Small Area FMRs are required to be used to set Section 8 Housing Choice Voucher payment standards in areas designated by HUD. Other Housing Agencies operating in non-designated metropolitan areas may opt-in to the use of Small Area FMRs. Furthermore, Small Area FMRs may be used as the basis for setting Exception Payment Standards – Public Housing Authorities (PHAs) may set exception payment standards up to 110 percent of the Small Area FMR. PHAs administering Public Housing units may use Small Area FMRs as an alternative to metropolitan area-wide FMRs when calculating Flat Rents.

Do your homework when setting rents; Use HUD's values as guideposts in your research.

# Please Support Our Sponsors



Home & Building  
Inspection Services, Inc.

**Bill Hughes, ACI**  
ASHI Certified Inspector  
NYS 1600000 7002  
CT HOI-0000091

845-897-5556  
518-833-0456  
Fax: 845-897-2498  
HabitatInspections@msn.com  
www.HabitatHomeInspection.com




**Renttropolis**   
Online Property Management Software

Take Control of Your Business  
For as Little as **\$9.97** a month

Start your free trial at  
[Renttropolis.com](http://Renttropolis.com)




**MACFAWN**  
FIRE & FLOOD RESTORATION



NYS Licensed Real Estate  
Salesperson and Real Estate  
Investor

**SEAN DALEY, CPA**



**SERENITY**  
REAL ESTATE TEAM

(518) 390-0578  
yourdaleyinvestor@gmail.com  
www.serenityrealestate518.com

**STUFF  
BREAKS.**

**SIGN UP AND SAVE**

Recurring Commercial  
and Residential Services

- 100% Tax Deductible
- All Building Trades Performed
- Fast Response Guarantee
- One Invoice per Month
- Monthly Summaries
- Satisfied Tenants
- Included Materials
- Concise Work Summaries
- Discounts for Larger Projects

**CALL US TODAY:  
518.833.3555**

[www.mktready.com](http://www.mktready.com)



**50% OFF  
FIRST MONTH**



market  
ready  
Property services llc

Commercial membership dues and sponsorships will vary based on desired advertisement formats. Please visit our [website](http://www.cdarpo.org) for more information.

# Handout on Identity Theft and Cybercrime Prevention

By Jeff Lanza

# Simple Safeguards: How to Stay Safe From Identity Theft and Cybercrime

Presented by Retired  
FBI Special Agent Jeff Lanza  
jefflanza@thelanzagroup.com;  
www.thelanzagroup.com

*About the presenter:* Jeff was an FBI Special Agent for over 20 years, during which he investigated cybercrime, organized crime, human trafficking, and terrorism. Jeff has lectured at Harvard and Princeton Universities and written two highly reviewed books. He is featured in a Netflix documentary about the FBI and he often appears on national television news programs where he talks about the growing threat of cybercrime.

Here's an executive summary of the presentation with more details on the following pages:

## 1. Prevent Identity Theft

### Create an online social security account

With your social security number and other personal information, a criminal can sign-up for social security benefits in your name and have the benefits sent to them. Here is what to do: If you are 62 years-of-age or older and have not created your online social security account, prevent a criminal from doing it before you. Sign-up at [www.ssa.gov](http://www.ssa.gov).

### Freeze your four credit reports

A freeze restricts access to your credit reports and should prevent new accounts from being opened in your name. You will have to lift the freezes before you can open a new account. Freezing is highly recommended and is a proven way to protect against new account fraud. To freeze your credit reports, see the contact information of the reporting agencies on the next page.

### Protect your paper

Shred your sensitive trash with a cross-cut, micro-cut or diamond-cut shredder. Don't leave outgoing mail with personal information in your mailbox for pickup. Consider signing-up for e-delivery of all your financial statements, as this is the more secure way to have documents delivered.

## 2. Watch Out for Tricks

### Covid scams

Criminals mutate their methods and try to take advantage of current vulnerabilities. Be wary of unsolicited phone calls, text messages and emails, especially having to do with Covid. You should not provide your social security number or money to people who contact under the guise of Covid, or any crisis.

### Account takeovers

As the term implies, account takeovers happen when someone gets unauthorized access to your online accounts. To prevent this, don't click on links or attachments in emails that you were not expecting or that don't make sense. Always log in to accounts by going directly to their websites, not through links.

### Wire transfer fraud

This occurs when a criminal tricks a victim into wiring money to their bank account. Most commonly, a real estate company's email account is hijacked by a hacker, which provides them with information about people who are about to close on a home purchase. Right before closing, the hacker sends an email from the hijacked account to the home buyer instructing them to wire money for the closing to the criminal's or a mule's bank account. It can be very difficult to recover this money if it is not discovered very quickly. The FBI reports that home buyers have lost hundreds of millions of dollars every year to this scam. It is important to verify wire transfers with the recipient by phone or in person before sending money.

## 3. Protect Your Computer

### Beware of pop-ups

Be cautious of pop-ups. Examples include ones that say you have to download something to see a video or a message that says there are threats detected on your computer. Don't click on anything in these pop-ups, including the "X" inside the pop-up itself. To remove the pop-up safely, hold down three keys: CTL+ALT+DEL (Windows) or CMD+Option+Escape (Mac). Then run your antivirus software to see if there is malware on your computer that caused the pop-up.

### Keep your software updated

To stay safe from the latest threats, make sure that your operating system software and antivirus software is updated automatically. This can be configured in the settings/security options. Mobile device software should be kept updated as well.

### Use passphrases instead of passwords

A passphrase is composed of a combination of words strung together. Passphrases protect us against two hacks the criminals use to gain access to our accounts. First, **brute force attacks**, where hackers use powerful programs and computers to guess passwords. Second, **credential stuffing**, where a hacker obtains a password for one site and uses it to hack another site. It's a two for one special! Strong passwords will also keep us safe against these threats, if you use a different one for each account, which unfortunately, not all of us do. See page four in this document for more information about passphrases.



# Preventing Identity Theft

## Protect Your Social Security Number

- ✓ Don't provide your social security number to anyone unless there is a legitimate reason, which include occasions when you are applying for employment, opening a financial account, freezing your credit reports or if someone is conducting a background investigation on you. Your doctor does not require your social security number for medical services.
- ✓ The Social Security Administration does not contact people by phone. If you receive a phone call purporting to be from them, it is most likely a trick to get you to provide your social security number.
- ✓ Don't routinely carry your social security card or any document on which it is printed with you.
- ✓ If someone that you contact asks you to verify the last four digits of your social security number, that's okay.

## If a criminal steals an identity, here are six things they can do - and how you can stay safe:

①

### They open credit card accounts, bank accounts and loans in your name.

**Prevention:** Freeze all four of your credit reports. A freeze restricts access to your credit reports and should prevent new account activity in your name. Once frozen, you must lift the freeze before you can get new credit. Freezing is highly recommended and is a proven way to protect against new account fraud. Below is the contact information for the agencies.

**Experian:** (888) 397-3742 | P.O. Box 9530 Allen, TX 75013 | [www.experian.com/freeze](http://www.experian.com/freeze)

**Equifax:** (800) 685-1111 | P.O. Box 740241 Atlanta, GA 30374 | [www.equifax.com/personal/credit-report-services](http://www.equifax.com/personal/credit-report-services)

**Innovis:** (800) 540-2505 | P.O. Box 1640 Pittsburgh, PA 15230 | [www.innovis.com/personal/securityfreeze](http://www.innovis.com/personal/securityfreeze)

**Trans Union:** (888) 909-8872 | P.O. Box 2000 Chester, PA 19016 | [www.transunion.com/credit-freeze](http://www.transunion.com/credit-freeze)

Keep your credit reports frozen indefinitely. You can freeze credit reports by mail, phone or online. It's easiest to do it online. When freezing, you will create a PIN, which is needed to lift the freeze when necessary.

### Before you freeze your credit reports, it's a good idea to check them for unusual activity.

You are allowed four free reports each year. To order three: [www.annualcreditreport.com](http://www.annualcreditreport.com) or 877-322-8228;  
Your credit report at Innovis must be ordered from: [www.innovis.com/personal/creditreport](http://www.innovis.com/personal/creditreport)

②

### They file state and federal tax returns in your name.

**Prevention:** For federal taxes, depending on where you live, you might be able to get a PIN from the IRS to prevent fraud. To see if you can, go to this site: [www.irs.gov](http://www.irs.gov). Check with your state authorities to see what methods they use to help prevent fraud. Victims won't be able to file tax return in the normal manner. But they still must pay their tax on time!

③

### They get medical care or prescription drugs in your name.

**Prevention:** Notify your medical insurance provider if you have been a victim of any other form of identity theft. Check your health insurance statements carefully. If a criminal uses your identity to receive medical services, not only does it defraud the insurance provider, but it could create entries in your permanent medical record for procedures you did not receive and conditions that you don't have.

④

### They file for social security benefits in your name (if you're eligible.)

**Prevention:** Create an online social security account at [www.ssa.gov](http://www.ssa.gov). When you create an online account, it does not mean that you have to collect benefits, just that a criminal can't do that in your name. Note that you can create your online account at any age and track your benefits throughout your lifetime through this online portal.

⑤

### They file for unemployment benefits using your identity.

**Prevention:** There has been a large increase in fraudulent unemployment claims using stolen identities. Criminals filing for benefits using a stolen identity must have the personal information of the victim. It is important to be wary of telephone calls, text messages, letters, non-verified websites, or emails that require you to provide sensitive information, including birth dates and social security numbers. If you have become a victim, contact your employer and your state unemployment office to report the fraud and follow their instructions regarding resolution.

⑥

### They steal the identity of a deceased person

**Prevention:** Identity theft could happen after someone dies. A criminal may use a deceased person's details to drain accounts, set up new loans, steal government benefits and more. Here is what you should do: Get copies of the official death certificate and provide it to all four credit bureaus and the deceased's financial institutions.

### Other terms regarding credit reports and what they mean:

**Credit Monitoring:** Your credit reports are monitored and if activity occurs, you are notified. ***Inside Scoop:** Credit monitoring does not prevent fraud. It only notifies you when your credit reports have been accessed. In most cases, the monitoring companies provide other benefits such as help with resolution, which can be very beneficial.*

**Fraud Alert:** Your credit file at the four credit reporting agencies is flagged for 90 days or for seven years if you have already had your identity stolen. Creditors should take steps to verify the identity of a person opening a new account. ***Inside Scoop:** Not worth the effort. Fraud alerts only work if the merchant takes steps to verify the identity of the applicant.*

**Credit Lock:** Limits access to your credit reports by some parties without your approval. ***Inside Scoop:** Don't use this. Locks are not governed by federal law, there is no guarantee of error free operation and some credit reporting agencies may charge you a monthly fee for this service.*

### Steps to take if you are a victim of identity theft

1. Visit [IdentityTheft.gov](http://IdentityTheft.gov) to report and recover from identity theft. This site should provide you with a good plan to recover based on your personal situation. You may also need to take the following steps, if they are not included in the plan.
2. Check your credit reports for accounts that have been opened in your name.
3. Notify those organizations of the fraud.
4. Freeze all four credit reports. You can freeze your reports by phone, mail or online.
5. Call your local police and file a report.
6. Call the Social Security Administration's fraud hotline at 800-269-0271.
7. Contact the Internal Revenue Service at 1-800-829-0433.
8. Contact your state taxing agency and follow their instructions to address the situation.
9. Notify any organization that has your money, including financial advisors.
10. Notify your medical insurance providers.

### Child identity theft

A child's social security number can be used by identity thieves to apply for government benefits, open bank and credit card accounts, apply for a loan or utility service, or rent a place to live. Check for a credit report to see if your child's information is being misused. If it is, visit [IdentityTheft.gov](http://IdentityTheft.gov) to report and recover from identity theft. Federal law allows you to create and freeze credit reports for children to keep them safe from potentially years of fraud.

### Social media and identity theft

**Personal information** - Information such as your full name (including your middle name), date of birth, hometown, pet names, interests and hobbies, nature of work, and home or office address are just some of the personal details that people post on their profile. Criminals can use these details to commit fraud. Protect this information to limit the risk of identity theft.

**Friend requests** - You should only accept friend request from people that you know. Some requests come from attackers, who then may share malicious links that lead to malware or phishing sites.

**Your posts** - By default, Facebook tends to make everything you put on it's network public. One quick way to lock down everything you post is to set your default sharing option to **friends** and not **public**. When you make this change, only your approved friends see your posts.

### Robocalls and identity theft

In many cases, robocalls are used to help facilitate identity theft. Be skeptical of your caller ID, as it could be spoofed by a criminal to make it look like the call is coming from a federal agency like the IRS or Social Security Administration. As a rule, don't give information to people who contact you by phone. To help to stop robocalls, you might consider **Robokiller**, a cell phone app and **Nomorobo**, which can be used for landlines connected to the internet.

### Identity theft and home title fraud

Criminals use your identity to forge paperwork which transfers your real estate into their name. The transfer is not legitimate, because it is based on fraudulent documents. However, it is possible they could sell the property before the fraud is discovered. Your best defense here is to routinely monitor your property's records in the county. Check with your county to see if they offer automatic notification if there is a record change.

### To remove your name from lists:

**Mail** - [www.dmachoice.org](http://www.dmachoice.org) **Phone** - [www.donotcall.gov](http://www.donotcall.gov)

**To stop credit card offers and other solicitations:**

[www.optoutprescreen.com](http://www.optoutprescreen.com) **or** 1-888-5-OPTOUT (567-8688)

### Key Resources

**Police or FBI:** Search online for local number  
**FTC:** 1-877-IDTHEFT; [www.identitytheft.gov](http://www.identitytheft.gov)

**To Report Internet Fraud:** [www.ic3.gov](http://www.ic3.gov)

# Preventing Cybercrime

Here is some more information about the tips that I discussed in the presentation.

## Protect Your Credentials

- To prevent account takeovers, it is important to protect your login credentials. Go to login pages directly, not through a link in an email or a pop-up.
- Before entering personal information, ensure you are on a secure site by looking for a lock icon at the beginning of the web address.
- Click on the lock to see a certificate, which verifies the authenticity of the site.
- For future access, store the site's web address in your browser's bookmarks or favorites.

## Hover to Discover

- Email addresses can be spoofed. Hold your mouse without pressing the button (hovering) over a sender in an email to see the true sender. If the two email addresses are different, then someone may be trying to trick you.
- Hovering also works with website links, so you can see where the link will re-direct you to if you click on it.
- If you see two letters before the first single slash in a website link, those letters refer to a country where the website is located. A foreign country code could indicate possible fraud.
- To preview a link on a mobile device, press and hold the link.

## Multi-Factor Authentication (MFA)

With MFA, you use a password **and** a PIN (most often sent to your phone) to log in to online accounts. This will help prevent an online account takeover. At a minimum, it should be used for financial accounts and email accounts. Most email providers won't ask for the code every time you log in if they recognize your computer and IP address.

## Software and Security

- It is imperative that Windows computers be protected with antivirus software. Popular options are **McAfee**, **Norton** and **Windows Defender**, which comes free with Windows 10.
- Keep in mind that these programs provide one layer of perimeter security. If malware evades them, they most likely won't be able to remove it because they couldn't stop it in the first place.
- You might consider a malware removal program that does search and destroy missions. A popular free program that is very effective is called **Malwarebytes**. The free version compliments your antivirus program. It does not replace it.
- Configure your settings so that your operating system software and antivirus software is updated automatically.

## Passphrases

A passphrase is like a password, only it's composed of a combination of words strung together. That makes them easier to create and remember. Here are some tips to make strong passphrases:

- Use at least twelve characters to protect against **brute force attacks**.
- Create a unique passphrase for each online account. This prevents **credential stuffing**.
- If a website makes you add complexity, you can add it to the passphrases that you have created.
- Here's an example passphrase for a Netflix account: *leavetheguntakethecannoli* 😊

## Passwords/Passphrases Managers

- Consider using a password manager to help keep track of all your unique passphrases. Some good options are **Keeper**, **Dashlane**, **1Password**, **LastPass** and **Bitwarden**.
- Another option is entering the passphrases in the note app on your smartphone and locking the note. This protects the contents of the note but keeps them assessable to you.

## Unsubscribing from Emails

If you receive unwanted emails from organizations that you are familiar with and/or have done business with, you should unsubscribe. Don't reply to or unsubscribe from spam because that notifies the sender that you have an active email address, which could result in more spam. Send these emails to your spam folder.

## Mobile Security

- Always use a passcode to protect your mobile devices. This keeps the information and apps more secure.
- Watch out for trick text messages. Don't call, click or reply unless you have verified the sender's authenticity.
- Download apps only from trusted sources. Make sure you check ratings and reviews if they are available and read the app's privacy policy to see exactly what personal information it will have access to if you download it.
- Don't give apps more permissions than they need for their purpose.
- Keep your operating system and apps updated. You can set you device to do this automatically in settings.
- Turn off Wi-Fi and Bluetooth when not needed. They announce your presence and are trackable by anyone interested.
- Delete unused apps from your mobile devices as they may have permission to access your personal information. Here's how for an **iPhone**: settings-general-iPhone storage-delete. For an **Android**: Settings-apps-uninstall.



### Home Wi-Fi Networks

- Change your Wi-Fi's default name to make it harder for hackers to know what type of router you have.
- Change the default username and password for your router. It's easy for hackers to guess it, especially if they know the manufacturer.
- Use a strong passphrase and WPA2 encryption.
- If you have children actively using Wi-Fi, you might have a separate router for them to keep **you** safer.

### Virtual Private Network (VPN)

Using an unsecured public Wi-Fi network could expose your private information. A virtual private network, better known as a VPN, creates a secure connection between your computer and the websites you are visiting. It is a must for accessing sensitive information in a public Wi-Fi network. Check the reviews on VPN options and get one that encrypts **all** of your traffic. Don't have a VPN? Use the cellular network on your phone to connect to the internet instead of the public Wi-Fi network.

## Common Cybercrime Scams

Below are some more details on some common cybercrimes and how you can stay safe.

### Fake Emails

- Be careful where you click. Don't click on links or attachments in emails from an unknown sender, a suspicious sender or in emails that don't make sense.
- Remember that a friend's email account can become compromised and that attackers can "spoof" someone's email address to appear to be from anyone.
- Don't react emotionally to an email. The hackers count on this to overcome logic and common sense to try to convince us to make bad decisions.

### Email Account Takeovers

It is very important to protect email accounts from hackers. If they get access to an email account, they can use it as a base for committing fraud that could affect more than one person or account. For example, they might be able to:

- Log in to other accounts if the victim uses the same username and password.
- Send malware or links to fake login pages to your contacts, who think the email is coming from you.
- Send wire transfer requests to a financial advisor.

### Tech Support Scams

Tech support scammers lure you with a pop-up window that appears on your computer screen that looks like an error message from your operating system or antivirus software. The message warns of a security issue on your computer and provides a phone number to get help. They want you to pay for tech support you don't need or to fix a problem that doesn't exist. They often want payment by gift card because it can be hard to reverse. They may ask for remote access to your computer. If someone calls you with this schtick, hang up and if you get a pop-up as described, don't call the number in the pop-up.

### Email Extortion Scams

According to the FTC, this scam has increased recently. In this scenario, the scammers lie and say they have access to your computer, webcam or have installed clever software to hack your files. They threaten to release personal information about you and your online habits if you don't pay them. But they may really know one of your old – or recent – passwords and they include it in the message to prove it. Most likely, this was obtained through a third part breach. When you see that, you know it's time to update your password on that account. If you get a message like this, don't engage with them and report the incident to the FTC at [www.FTC.gov/Complaint](http://www.FTC.gov/Complaint).

### Ransomware

**What it is:** Ransomware is a form of malware that restricts access to data by encrypting files or locking computers.

**How it begins:** Victims will open an email addressed to them and may click on an attachment that appears legitimate, like a notification of a missed package delivery. This may cause ransomware code to install on their computer.

**What happens next:** The malware encrypts files on a victim's computer. They see computer messages advising them of the attack and demands for a ransom payment in exchange for a decryption key to unlock a computer or recover the files.

**To stay safe:** Don't download attachments from an unknown source. Backup your files. But because ransomware can attack backups, using a cloud backup that can restore to previous versions that are not encrypted is a good option.

### Real Estate Wire Transfer Fraud

It begins when a criminal hijacks the email account of lawyers, real estate agents, title companies or lenders to get the details of real estate transactions about to close. Then, posing as a party to the transaction, the criminal will email a buyer with instructions on where to wire money for the closing. The buyer, who believes they have received legitimate instructions, will wire the money to the criminal. A wire transfer is almost impossible to reverse once completed. This crime is an epidemic and growing. Not buying a home? Warn family and friends who are. You might save them thousands of dollars in losses.

**There is too much money at stake for you to make a mistake. Here are some tips to stay safe from this crime:**

Know that wiring instructions rarely change and be very suspicious of last-minute wiring changes. During a real estate transaction, know the phone numbers of all the parties and know their voice. Get the wiring information in person or over a verified phone number. Finally, if your gut is telling you something is wrong, investigate. You are probably right.