

# **SCAMS 101:**

## **HOW TO AVOID CURRENT INTERNET AND PHONE SCAMS**

**PRESENTED BY SALENA COLLER, COMMUNITY LIBRARY  
MANAGER OF THE GALT OCEAN MILE READING CENTER  
AND THE IMPERIAL POINT BRANCH LIBRARY.**

**CREATED BY THE COMPUTER CENTER EMPLOYEES WORKING  
AT THE BROWARD COUNTY'S MAIN LIBRARY. UPDATED  
SEPTEMBER 2023**

# OVERVIEW

- Everyday cyber criminals are developing new ways to commit fraud, access sensitive personal information, and steal people's identities and money.
- This program will provide information about some of the current Internet and phone scams that have taken place within the last year.
- Learn how to avoid commons scams and what you should do if you are scammed.



# TOPICS

- Phishing Scams
- Bank & Tax Scams
- Scams happening with Broward County and the Library GPS Tracking
- COVID-19 Scams
- Phone Scams
- Library Scams
- Password Security
- Data Privacy
- What to do if you are scammed
- How to protect your computer and mobile devices
- Newsbank Database & Libby Magazines
- Contact & FAQ



# WHAT IS PHISHING

- **Goodwill Community Foundation** says, “Phishing scams are messages that try to trick you into providing sensitive information. These often appear to come from a bank or another trusted source, and they'll usually want you to re-enter a password, verify a birth date, or confirm a credit card number. Phishing messages may look real enough at first glance, but it's surprisingly easy for scammers to create convincing details.”
- Read the Goodwill Community Foundation's online article and watch the tutorial video about avoiding email spam and phishing scams: <https://edu.gcfglobal.org/en/internetsafety/avoiding-spam-and-phishing/1/>



- “Phishing” refers to the practice of attempting to trick the victim into giving sensitive information to the scammer. This information can be the password itself or information that a savvy person can use to unlock an account or reset a password. For example, a phisher might try to trick a person into revealing their bank password, or they may try to collect an account number, SSN, mother’s maiden name, etc. that they could use to “prove” the account holder’s identity” (AARP).

- Source: The American Association of Retired Persons. (2021, September). *Fraud Resource Center: Phishing*. AARP. Retrieved from: [www.aarp.org/money/scams-fraud/info-2019/phishing.html](https://www.aarp.org/money/scams-fraud/info-2019/phishing.html)

- The FBI reported that theft of roughly \$57 million can be traced back to phishing scams during 2019 alone (FBI Crime Report Staff).
- Source: Federal Bureau of Investigations. (2020, February). *2019 Internet Crime Report Released: Data Reflects an Evolving Threat and the Importance of Reporting*. FBI. <https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120>

## PHISHING: WHAT IS IT?





# PHISHING: IRS AND VENMO SCAMS

- Every year during tax season scammers attempt to phish people through spoofed letters and messages from the IRS promising extra refund money or threatening a fake audit (Tompur).
- Phishing attempts can pretend to be from payment programs such as Venmo, trying to get access to the keys to access a bank account or credit card through that program (Kenney).
- People claiming to be from Geek Squad or similar installation/repair services will claim that the victim owes them money for an old job and demand payment information (Baker).
- Sources:
  - Baker, L. (2021, April 21). "A Hacker's Brief: Avoid These Scams." *Wyoming Star Tribune*.
  - Kenney, T. (2021, March 11). "Did You Get Paid By 'Accident' on Venmo? It Could Be a Scam, Watchdog Group Warns." *Miami Herald*.
  - Tompor, S. (2021, March 11). "Taxes – Tax Time is Also Scam Time. Here's How to Avoid Being Caught in a Fraud." *Miami Herald*.



# PHISHING SCAMS

## REAL EXAMPLES:

RE: All storage used.  
Upgrade to keep personal  
files

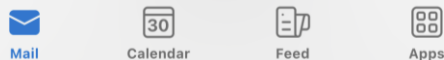
 **STORAGE\_GOOGLE**  
info@filame.com

To: You   
Monday, August 28, 4:14 PM

[Get your FREE storage today!](#)



Reply



You have reached your storage limit



Dear customer,  
Your Google storage is full.

As a result, you may not be able to upload new files to Google Drive  
and Google Photos. But, as part of your loyalty program, you can now  
receive an additional 50 GB for free before the files on your Google  
Drive are deleted.

[Get FREE Storage](#)

\* After signing up, you have to insert your credit card details for validation of your Gmail ID.  
We will not withdraw any amount.

To stop these please go [here](#) write to:  
616 Corporate Way Ste.2-9092  
Valley Cottage, NY 10989

Reply



RE: Your Solution For Covid  
Recovery

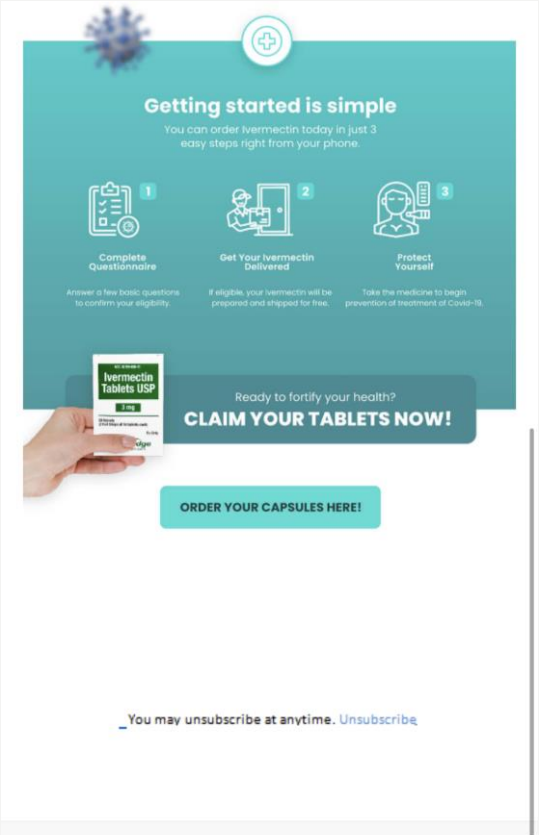
 **Ivermectin Affiliate**  
sales@chouchoute.co...

To: You 

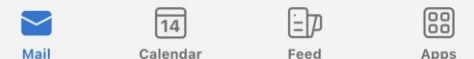
Thursday, September 14, 6:4



Reply

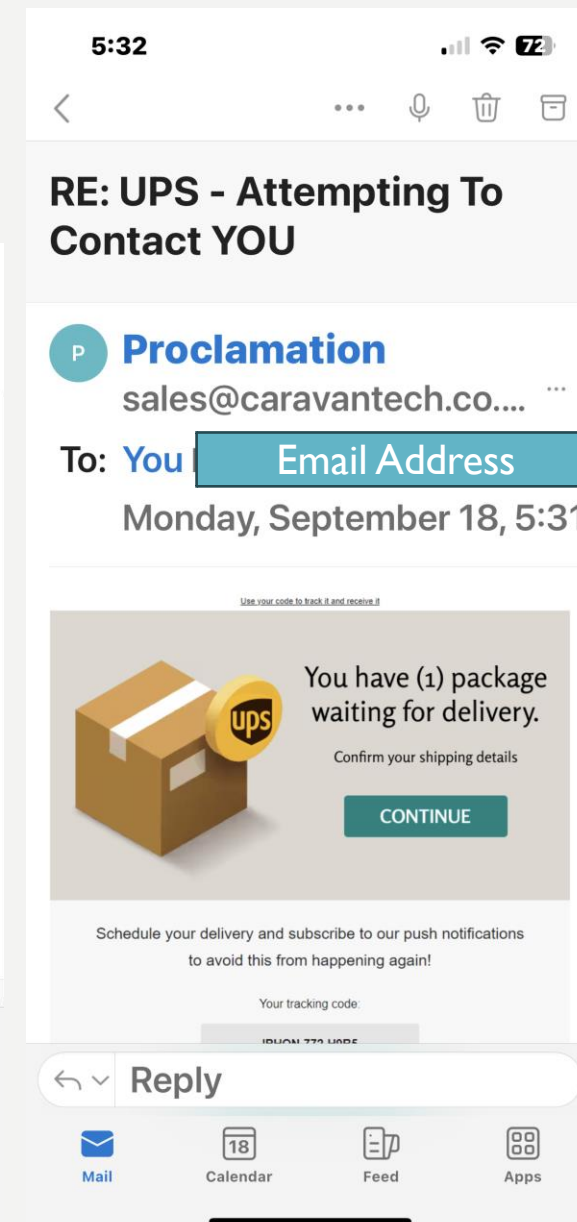
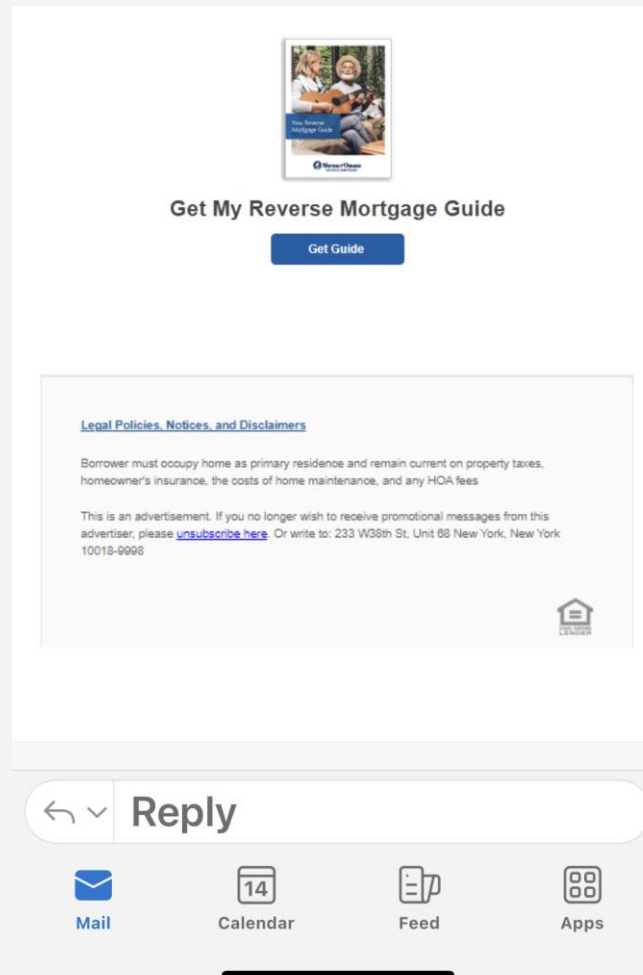
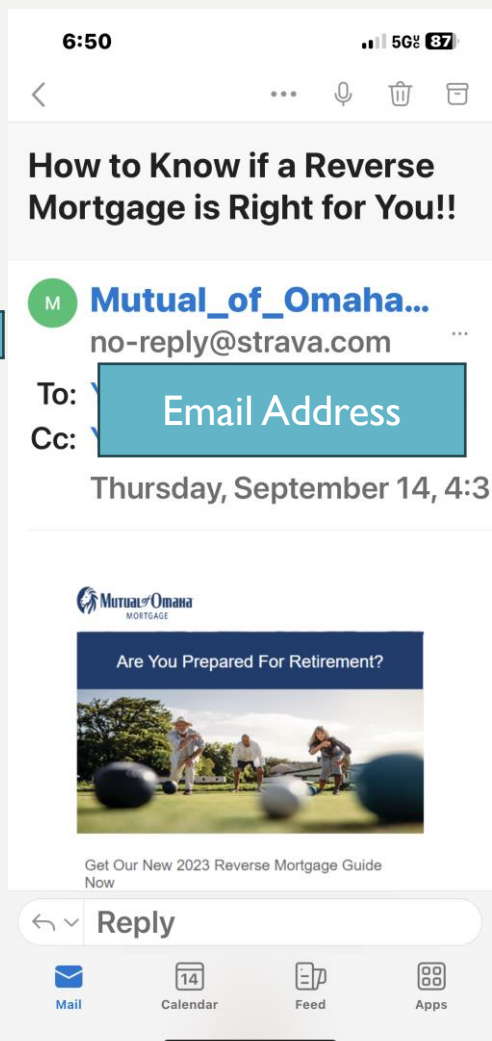
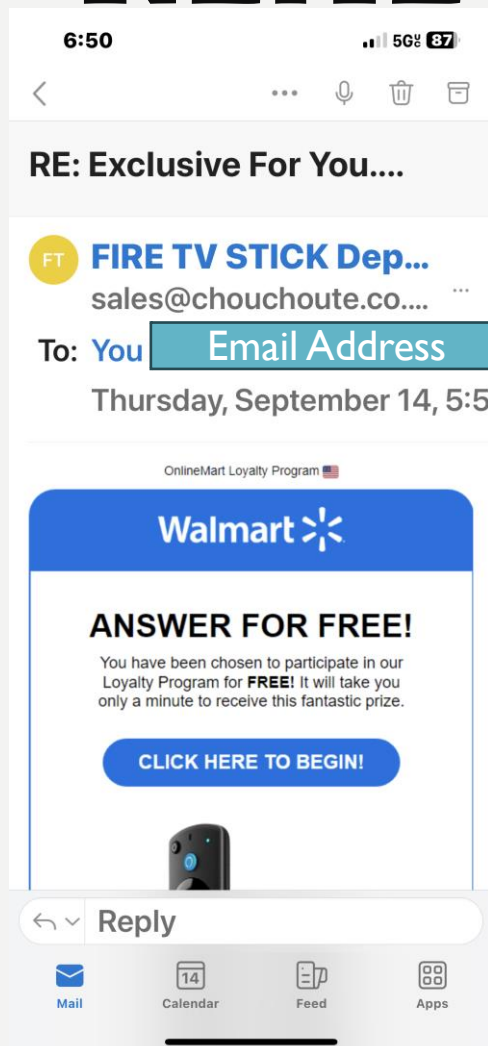


Reply



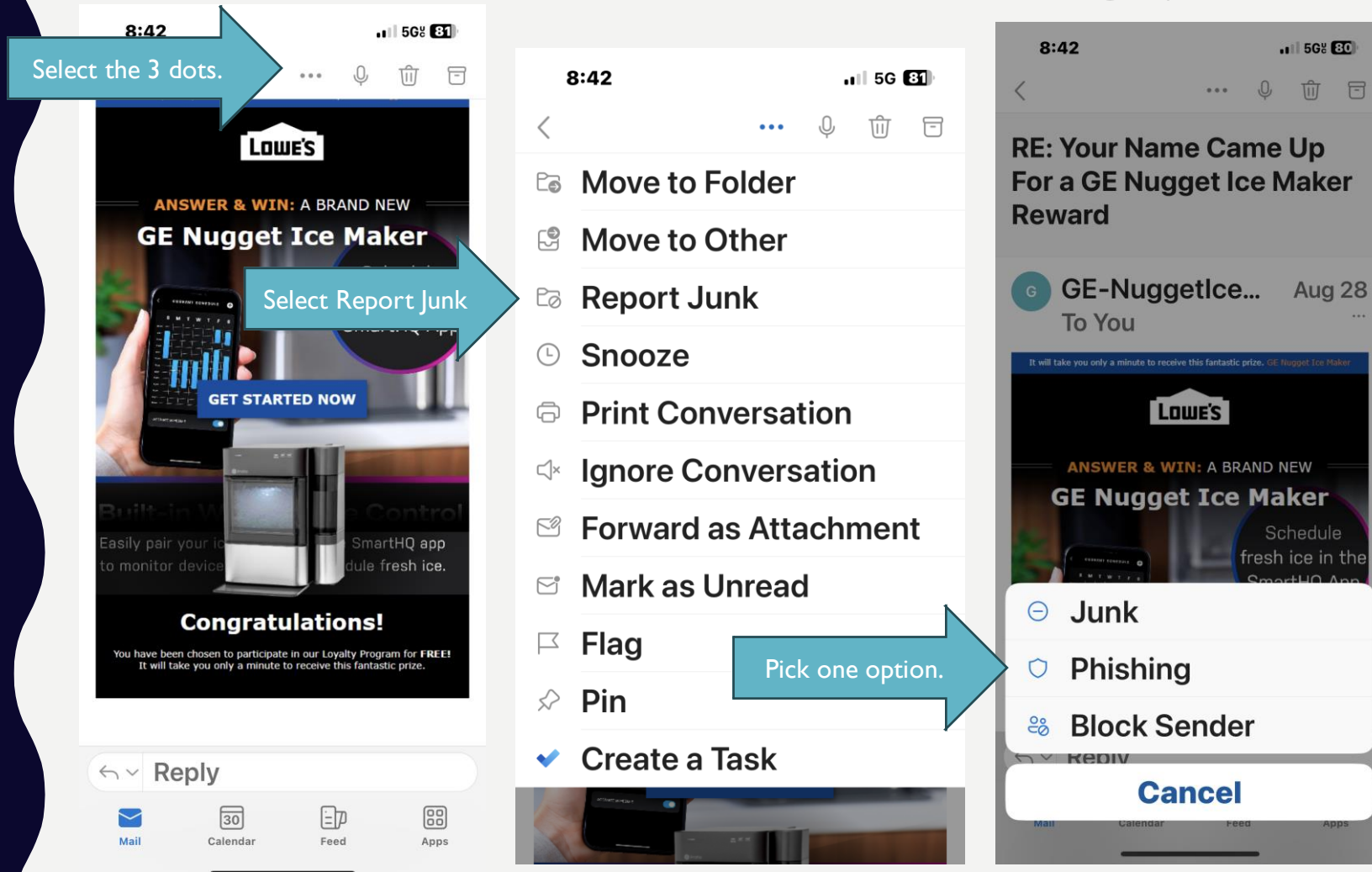
# PHISHING SCAMS

## REAL EXAMPLES:

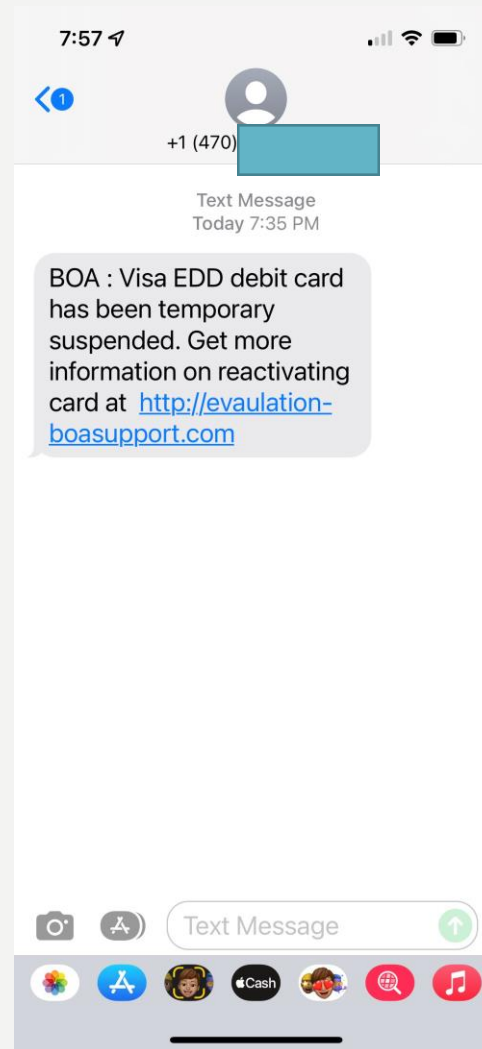
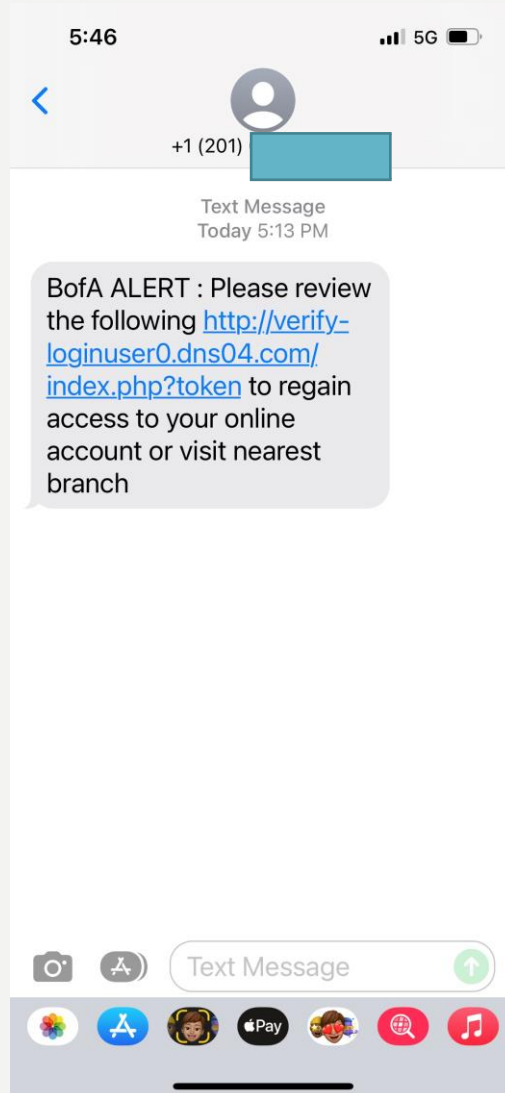




# PHISHING SCAMS REAL EXAMPLES:



# BANK SCAMS



- Bank imposter scam:
- [www.wellsfargo.com/privacy-security/fraud/bank-scams/bank-imposter/](http://www.wellsfargo.com/privacy-security/fraud/bank-scams/bank-imposter/)
- Scams and Cyber Threats:  
[www.wellsfargo.com/privacy-security/fraud/bank-scams](http://www.wellsfargo.com/privacy-security/fraud/bank-scams)

# TAX SCAMS



- **The Dirty Dozen represents the worst of the worst tax scams:**  
[Dirty Dozen | Internal Revenue Service \(irs.gov\)](https://www.irs.gov/privacy-disclosure/report-phishing)
- “Compiled annually, the “Dirty Dozen” lists a variety of common scams that taxpayers may encounter anytime but many of these schemes peak during filing season as people prepare their returns or hire someone to help with their taxes. Don’t fall prey” (IRS.gov).
- The IRS does not use social media applications, email and text messages to contact taxpayers about personal income tax issues (IRS.gov).
- “The IRS doesn't **initiate** contact with taxpayers by email, text messages or social media channels to request personal or financial information. This includes requests for PIN numbers, passwords or similar access information for credit cards, banks or other financial accounts” (IRS.gov).
- **Report Phishing and Online Scams** - Find more information here: <https://www.irs.gov/privacy-disclosure/report-phishing>
- Once you have determined that it is not legitimate, report the incident to [TIGTA](#) and to us at [phishing@irs.gov](mailto:phishing@irs.gov) (IRS.gov).

# TAX HELP

- **Need help visit:**  
[IRS Videos on YouTube](#)
- **The Official IRS Website:**  
[Internal Revenue Service | An official website of the United States government \(irs.gov\)](#)
- **Broward County Tax Assistance Information:**
  - Broward Tax Pro
  - AARP Foundation Tax Aide Program
  - MyFree Taxes
  - IRS - Free Tax Preparation



Image: Pixabay (2022). Retrieved from <https://pixabay.com/photos/income-tax-calculator-accounting-4097292/>



# SCAMS IN BROWARD COUNTY

- **“I received a phone call from someone identifying themselves as the Broward County Tax Collector who requested financial information from me to pay my taxes over the telephone. Is this an acceptable way to pay my taxes?”**
- ***Answer: No! Beware of any call you receive encouraging you to pay your taxes over the telephone. The Broward County Tax Collector will never call a taxpayer to solicit over-the-phone payments of current and/or delinquent taxes. Tax payments cannot be made over the phone***
- Source & frequently asked questions about property taxes:  
[www.broward.org/RecordsTaxesTreasury/FAQs/Pages/PropertyTaxes.aspx](http://www.broward.org/RecordsTaxesTreasury/FAQs/Pages/PropertyTaxes.aspx)

## Consumer Alerts: Important Information for Residents

- Some Broward County homeowners are receiving letters from private companies selling them certified copies of their deeds at premium prices. County residents are also receiving similar unofficial home warranty service advertisements via postcards. These companies are not affiliated with Broward County nor does the County provide home warranty services.
- The Records, Taxes and Treasury Division provides County property owners official documents at little or no cost. Save money by clicking [here](#).
- County residents are also being charged premium fees by private companies for Auto Tag and Registration documents. Our Division can save you money with getting these official documents by clicking [here](#).
- Information Source:  
[www.broward.org/RecordsTaxesTreasury/Pages/Default.aspx](http://www.broward.org/RecordsTaxesTreasury/Pages/Default.aspx)

# GPS TRACKING

- Some of Apple's small AirTag tracking devices which are typically used to locate lost keys and items are being used for illegal purposes such as stalking someone or carjacking (Marnin, 2021).
- Source: Marnin, J. (2021, December 23). *If you get this apple alert on your phone call 911, cops say.* *Miami Herald*. Retrieved April 11, 2022, from <https://www.miamiherald.com/news/nation-world/national/article256816032.html>
- “For Android phone users, West Seneca police suggest downloading the Apple “Tracker Detect” app from the Google Play store to scan for any AirTag trackers potentially nearby.” Read more at: <https://www.miamiherald.com/news/nation-world/national/article256816032.html#storylink=cpy>



Image: Pixabay (2022). Retrieved from <https://pixabay.com/photos/google-maps-location-gps-map-3337030/>

# COVID-19 SCAMS: PHONE AND TEXT MESSAGES

- *"Real contact tracers will not ask for money. They will not ask for your Social Security number or your bank or credit card numbers. They also won't ask your immigration status".*

— Lisa Schifferle

Consumer Financial Protection  
Bureau, Office for Older Americans

## Contact tracing call?

### 5 things to know

A contact tracer from your state health department might call if you've been exposed to COVID-19. But scammers are pretending to be contact tracers, too. Here's how you can spot the scam.



**Real contact tracers won't ask you for money.**  
Only scammers insist on payment by gift card, money transfer, or cryptocurrency.



**Contact tracing doesn't require your bank account or credit card number.**  
Never share account information with anybody who contacts you asking for it.



**Legitimate contact tracers will never ask for your Social Security number.**  
Never give any part of your Social Security number to anyone who contacts you.



**Your immigration status doesn't matter for contact tracing, so real tracers won't ask.**  
If they do, you can bet it's a scam.



**Do not click on a link in a text or email.**  
Doing so can download malware onto your device.

Talking to a real contact tracer helps stop the spread of COVID-19. Reporting scammers helps stop them, too. Report fake contact tracers to your state and at [ftc.gov/complaint](https://ftc.gov/complaint).



FEDERAL TRADE COMMISSION

For more information about contact tracing visit your state health department's website and [ftc.gov/coronavirus/scams](https://ftc.gov/coronavirus/scams)

# COVID-19 SCAMS: PHONE AND TEXT MESSAGES

- The FBI says con artists are [advertising fake COVID-19 antibody tests](#) in hopes of harvesting personal information they can use in identity theft or [health insurance scams](#).
- Scammers claim to be selling or offering in-demand supplies such as [masks](#), test kits and [household cleaners](#), often in robocalls, texts or social media ads. The FTC has issued warnings to companies suspected of abetting [coronavirus robocalls](#), and the Federal Communications Commission (FCC) set up a [dedicated website](#) ([www.fcc.gov/covid-scams](http://www.fcc.gov/covid-scams)) with information on COVID-19 phone scams.





# COVID-19 SCAMS: EMAIL

- Be wary of third-party sources spreading information about COVID-19. Refer to the official CDC gov website for updates on the virus: [www.cdc.gov/coronavirus/2019-ncov/index.html](https://www.cdc.gov/coronavirus/2019-ncov/index.html)
- The Department of Justice issued an alert in late March about phishing emails and [text messages](#) disguised as [surveys about COVID-19 vaccines](#), purportedly sent out by shot producers [Pfizer, Moderna](#) and [AstraZeneca](#) and promising a "free" reward if you provide bank or credit card information to cover a small fee.



# COVID-19 SCAMS: ON THE INTERNET

- [Exercise caution if you are asked for a fast digital payment](#). The Venmo app, for example, points out that it is intended for use only between friends and others they trust. The same applies to similar apps.
- The FTC and the U.S. Food and Drug Administration (FDA) have sent [dozens of warnings](#) to companies selling unapproved products they claim can [cure or prevent COVID-19](#).
- Teas, essential oils, cannabinal, colloidal silver and intravenous vitamin-C therapies are among supposed antiviral treatments hawked in clinics and on websites, social media and television shows as defenses against the pandemic.



- The pandemic has brought about "significant increases in broad-based and targeted phishing campaigns," according to a July 30 alert from the Treasury Department's Financial Crimes Enforcement Network (FinCEN).
- Since January 2020, tens of thousands of new website domains have been registered with terms related to COVID-19 and the response to it, such as "quarantine," "vaccine" and "CDC," FinCEN says. The Justice Department has [shut down hundreds](#) of these suspect sites, which promise vaccines and other aid, often in the guise of government agencies or humanitarian organizations.
- If you contact one of those malicious domains, you could start getting phishing emails from fraudsters in an attempt to get personal information from you directly, or to plant [malware](#) that digs into personal files on your computer, looking for passwords and other private data for purposes of identity theft.

## COVID-19 SCAMS: ON THE INTERNET



# COVID-19 SCAMS: RESOURCES FOR MORE INFORMATION

- Scams will follow new COVID-19 rescue plan (US Federal Trade Commission) :  
[www.consumer.ftc.gov/blog/2021/03/scams-will-follow-new-covid-19-rescue-plan](https://www.consumer.ftc.gov/blog/2021/03/scams-will-follow-new-covid-19-rescue-plan)
- COVID-19-Related Phone Scams and Phishing Attacks (Centers for Disease Control): [www.cdc.gov/media/phishing.html](https://www.cdc.gov/media/phishing.html)
- Contact Tracing Call? Five things to Know (PDF):  
[www.ftc.gov/system/files/attachments/coronavirus-advice-consumers/contact\\_tracing\\_scams\\_infographic-1-508.pdf](https://www.ftc.gov/system/files/attachments/coronavirus-advice-consumers/contact_tracing_scams_infographic-1-508.pdf)
- 10 Red-Hot COVID Scams Vexing Older Americans (AARP Resources):  
[www.aarp.org/money/scams-fraud/info-2021/covid-19-scams-vexing-older-americans.html](https://www.aarp.org/money/scams-fraud/info-2021/covid-19-scams-vexing-older-americans.html)





# PHISHING: METHODS TO PROTECT YOURSELF INCLUDE

- Have different passwords for different accounts. If someone phishes one password, then they can only use it for one account instead of multiple accounts (AARP).
- Verify the source of messages. If a message claims to be from the IRS or from a company that you do business with, check the phone number or email to make sure it is genuine before giving them any sensitive information. Watch out for obscured phone numbers/e-mails or generic e-mail domains like Gmail or Protonmail (AARP).



# COMMON PHONE SCAMS: HOW DO I GET HELP?

- The Federal Trade Commission (FTC) received about 1.25 million fraud complaints in 2020 in which a contact method was identified, and in nearly 1 in 3 cases a call was the swindler's way in. Once they get you on the line, phone scammers use false promises, aggressive sales pitches and phony threats to pry loose information they can use to steal your money or identity (or both) (AARP).
- **Have you seen this scam?**
  - Call the [AARP Fraud Watch Network Helpline: 877-908-3360](tel:877-908-3360)
  - Report it on AARP's [Scam-Tracking Map](#)
  - Sign up for [Watchdog Alerts](#) for more tips on avoiding scams.
- Visit this site for more information:  
[www.aarp.org/money/scams-fraud/info-2019/phone.html](http://www.aarp.org/money/scams-fraud/info-2019/phone.html)



# COMMON PHONE SCAMS

- **Imposter scams:** Scammers pretend to be someone from a trusted organization like a government agencies, IRS, Social Security Administration, a family member, a romantic interest, or technology support. They will use a fake name or phone number that shows up on a person's caller ID.
- **Debt relief and credit repair scams**
- **Charity scams**
- **Extended car warranties**



# COMMON PHONE SCAMS PART 2

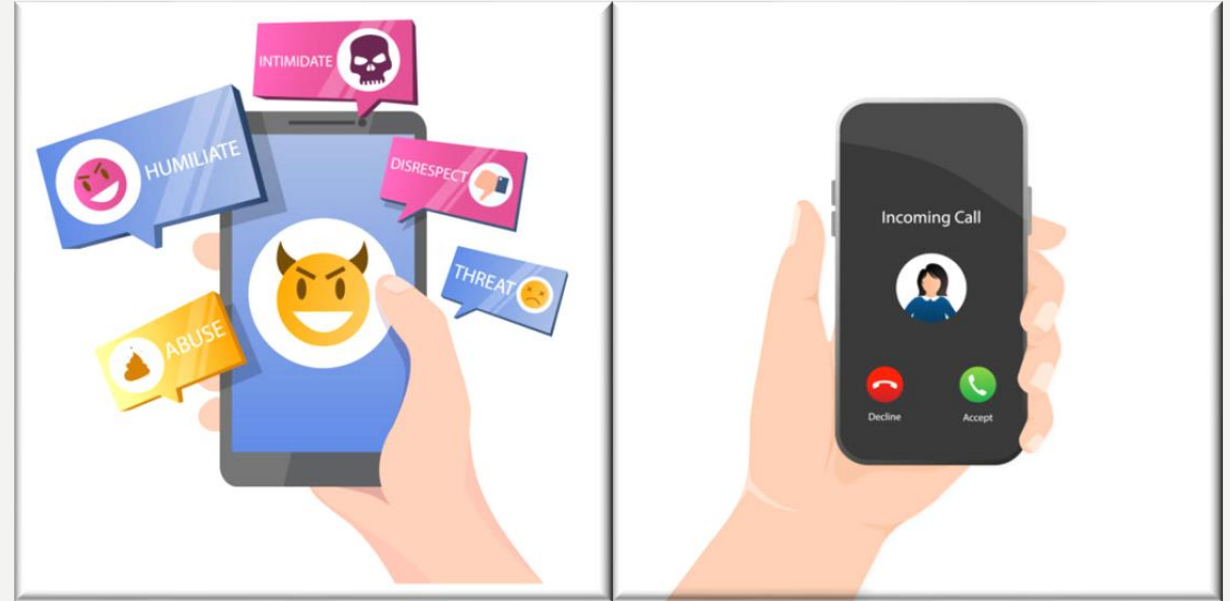
- “Free” Trials
- **Loan scams:** Callers target people with poor credit history and guarantee loans or credit cards if they are willing to pay an “up-front fee”. Legitimate lenders will not make those kinds of promises.
- **Prize and lottery scams**
- **Travel and timeshare scams**





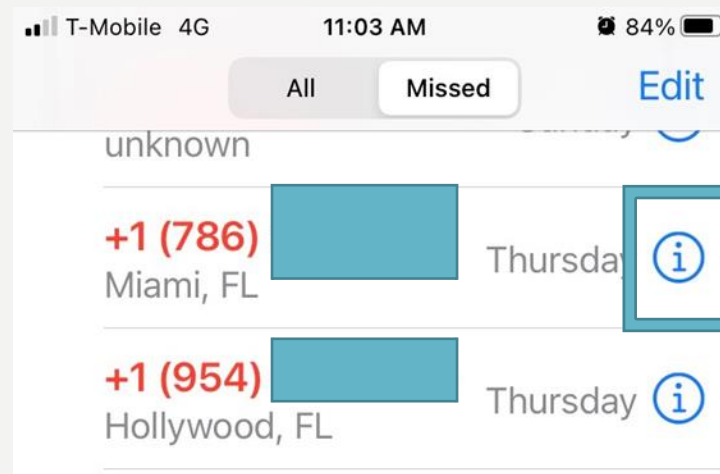
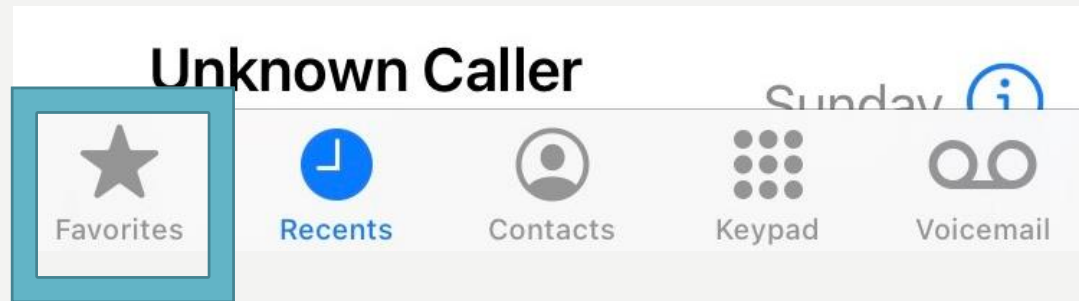
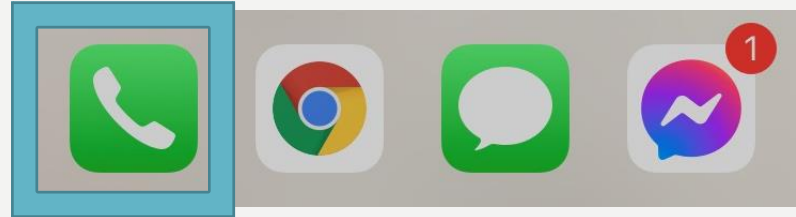
# HOW TO AVOID PHONE SCAMS

- Hang up the phone.
- Consider call blocking or call labeling.
- Don't trust your caller ID.



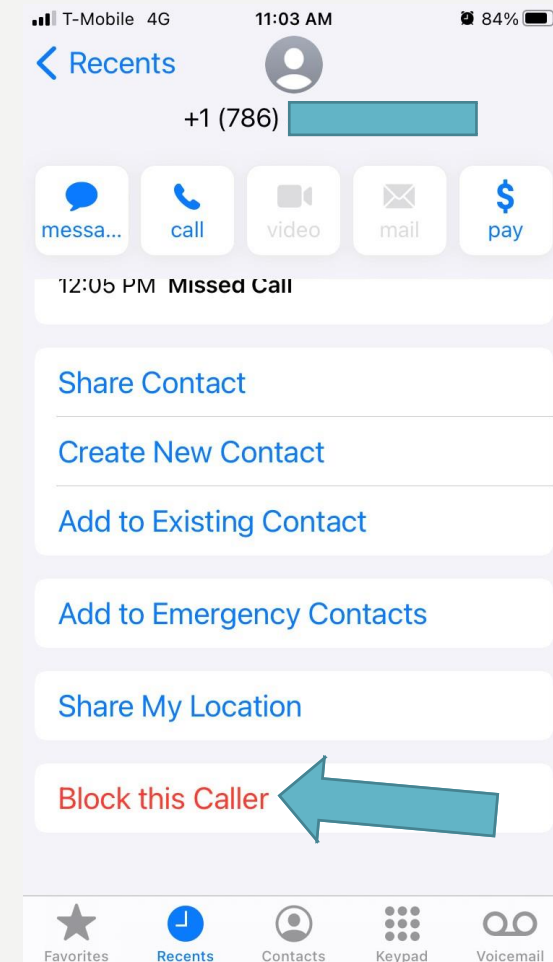
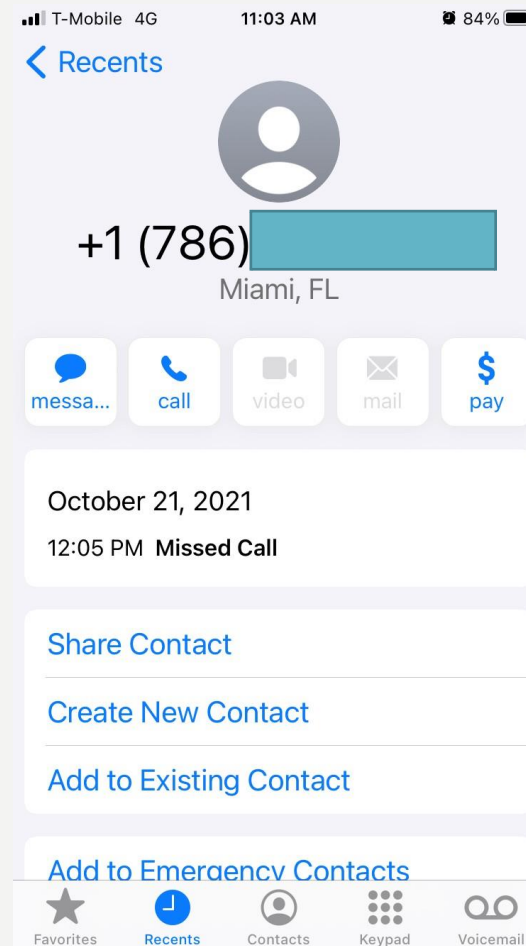
# BLOCKING SPAM CALLS ON AN IPHONE

- Please note that there are different versions of the iPhone operating system, so these steps may not be completely accurate. These screenshots are from an iPhone 8 (iOS 14.8).
- Select your **Phone icon** (green icon with white phone) >> **Recents** (clock icon).
- Select the “**I**” (information) icon.



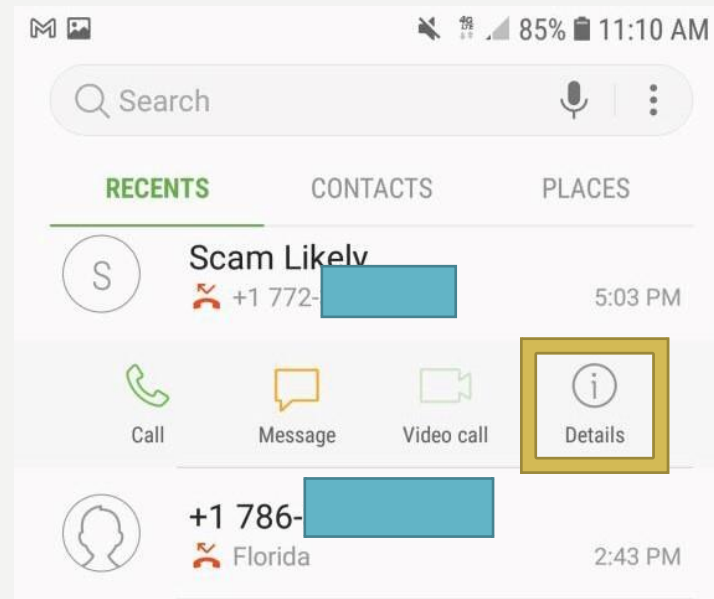
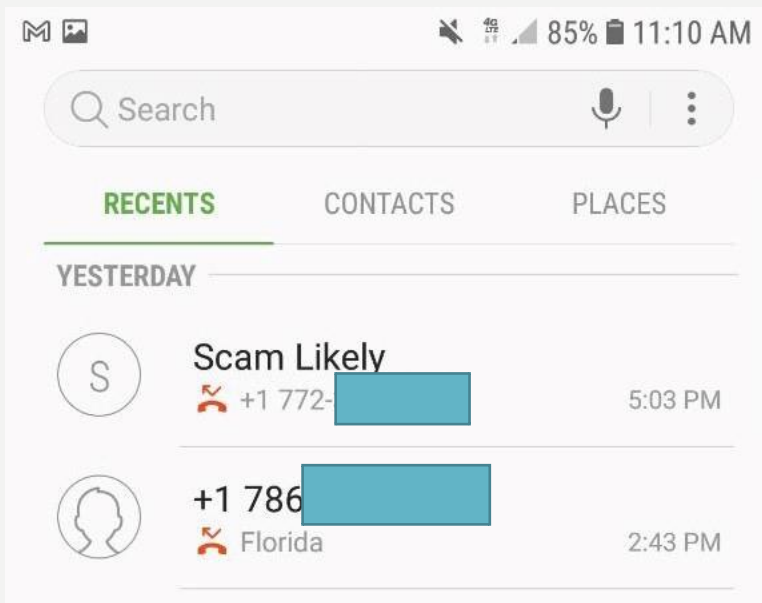
# BLOCKING SPAM CALLS ON AN IPHONE

- Please note that there are different versions of the iPhone operating system, so these steps may not be completely accurate.
- Scroll down and select **Block this Caller**.



# BLOCKING SPAM CALLS ON AN ANDROID PHONE

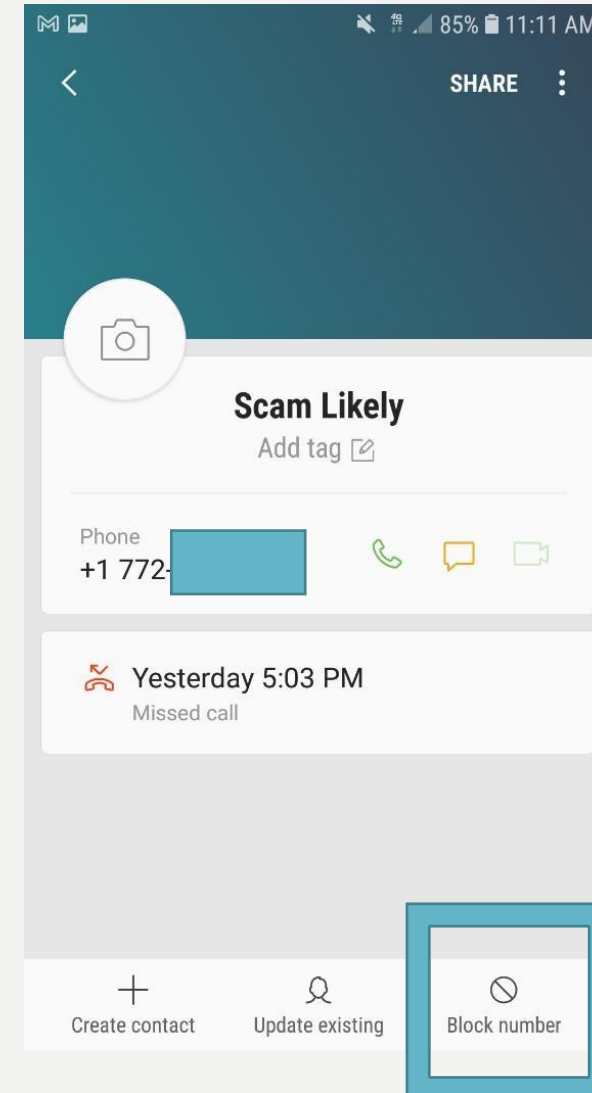
- Please note that there are different version of the Android operating system, so these steps may not be completely accurate. These photos are from an Android with operating system 8.0.
- If a call is labeled “**Scam Likely**” is a strong sign that the phone call is probably a spam call.
- Don’t answer the phone unless you know the caller or you are expecting a phone call from a new person or business.
- Select the **Details** option to block the phone number.





# BLOCKING SPAM CALLS ON AN ANDROID PHONE

- Please note that there are different version of the Android operating system, so these steps may not be completely accurate. These photos are from an Android with operating system 8.0.
- Notice there is an option to **Block number**.



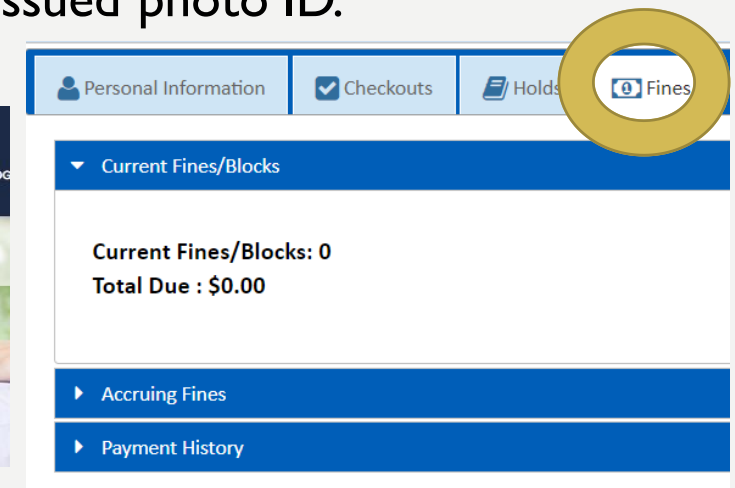
# LIBRARY RELATED SCAMS: TEXT MESSAGE SCAMS

- Around May and June 2022, library employees received inquiries from customers about text messages they have been receiving that claim that they owe libraries several hundred dollars.
- SirsiDynix has verified that there have been no data breaches and could not find any evidence that the text messaging system has been used to text these customers.
- These text messages are not originating from Libraries and that we would not text customers for overdue fines or for payment of bills.
- Bills are usually sent by mail to the customers.
- The texts these customers are receiving are probably a scam that Libraries across the United States and even Australia have reported.
- A message regarding this has been placed on our social media.
- Information about text message scams: [www.ftc.gov/business-guidance/blog/2020/02/text-message-package-scam-delivers-more-your-business-bargained](https://www.ftc.gov/business-guidance/blog/2020/02/text-message-package-scam-delivers-more-your-business-bargained)

# LIBRARY RELATED SCAMS



- Before responding to any library notices, log into your online account using the library's website or app. Website: [www.broward.org/library](http://www.broward.org/library), select **Login**, and then select **Fines** and/or **Checkouts**.
- If you are unsure about any library notifications, call your local branch and ask to speak with a circulation supervisor. Make sure to have your library card number available before you call.
- Visit your local branch in-person and speak with a circulation staff member or circulation supervisor. Make sure to bring your library card and government issued photo ID.



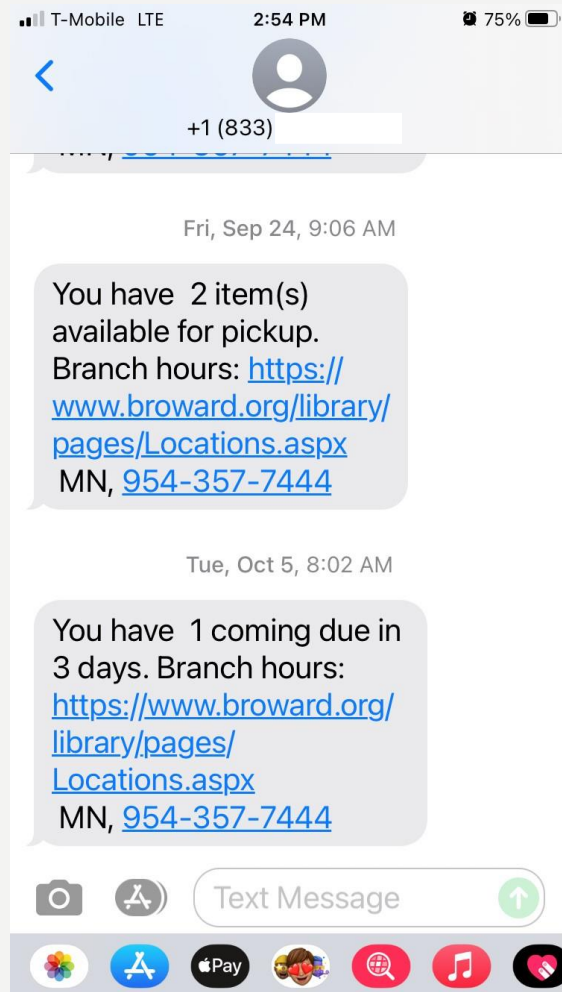
# LIBRARY RELATED SCAMS

- One library customer received an email from an unknown person using a **broward.com** domain within the email address which is not a domain Broward County Government uses.
- If you receive an email about overdue fines or notices, then double check the email address and make confirm that it is from a **broward.org** domain.
- Examples: [librarymarketing@broward.org](mailto:librarymarketing@broward.org), [cybrary@broward.org](mailto:cybrary@broward.org) or [periodicals@broward.org](mailto:periodicals@broward.org).
- The library will send overdue notices via automated telephone calls, text messages, postal mail, or email notification if you have provided the library with your current contact information.





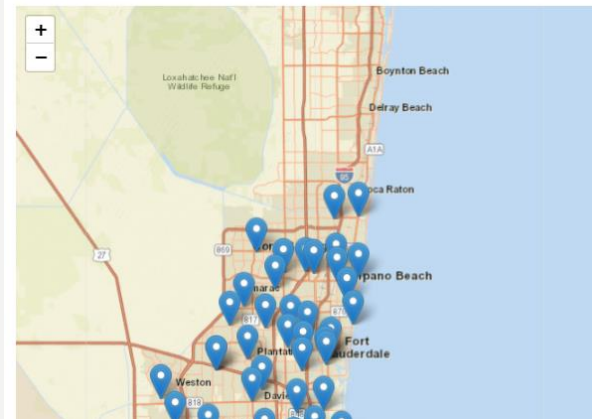
# EXAMPLES OF REAL LIBRARY TEXT NOTIFICATIONS



- The library website is listed [www.broward.org/library](http://www.broward.org/library)
- The library branch code. Example: MN = Main Library
- The Main Library's phone number: 954-357-7444 (Can be verified on the [www.broward.org/library](http://www.broward.org/library) website)

## LIBRARY BRANCH LOCATIONS

### Temporary Hours Holiday Closures



#### CLOSED NOW

[Get Directions](#)

#### Main Library | MN

954-357-7444  
100 S Andrews Avenue,  
Fort Lauderdale, FL 33301

Open Today Until 6:00PM

[Get Directions](#)

#### Margate Catharine Young Branch | MG

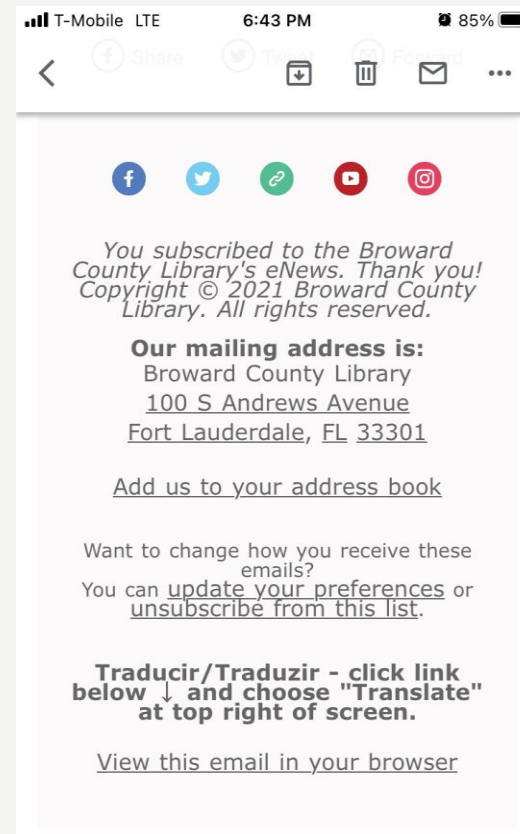
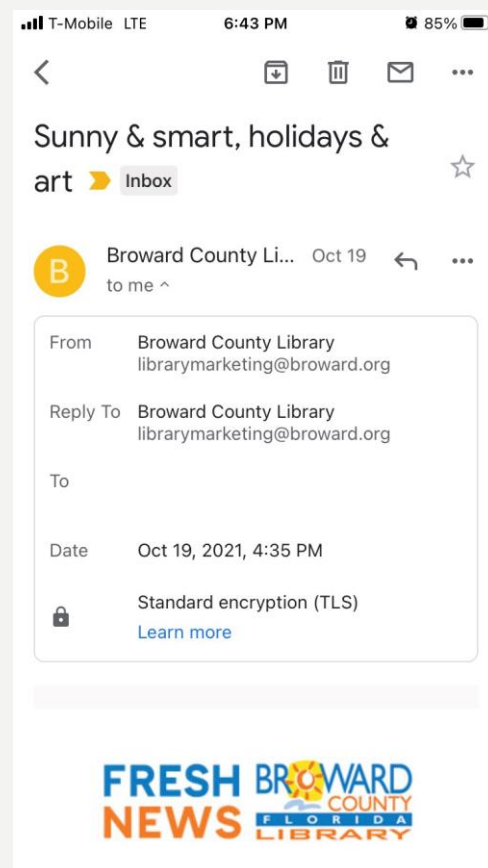
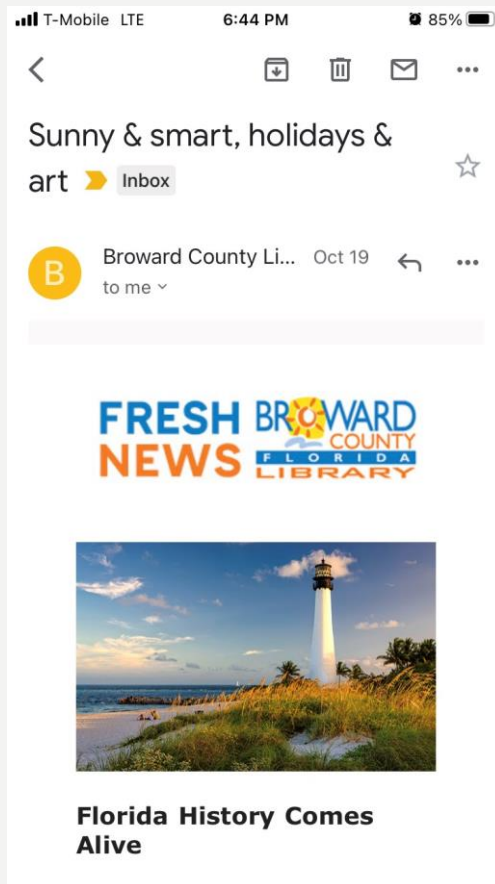
954-357-7500  
5810 Park Drive,  
Margate, FL 33063

CLOSED NOW

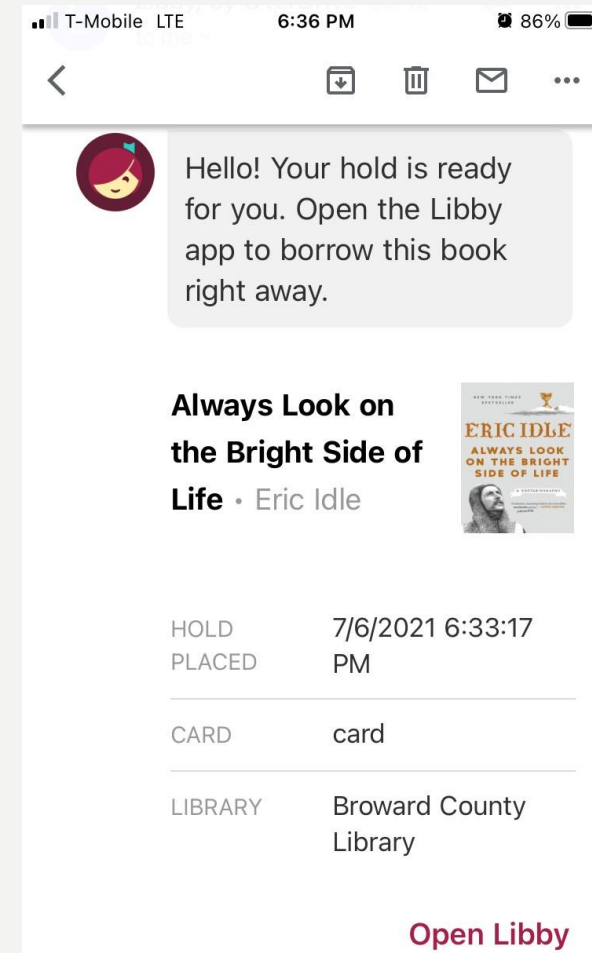
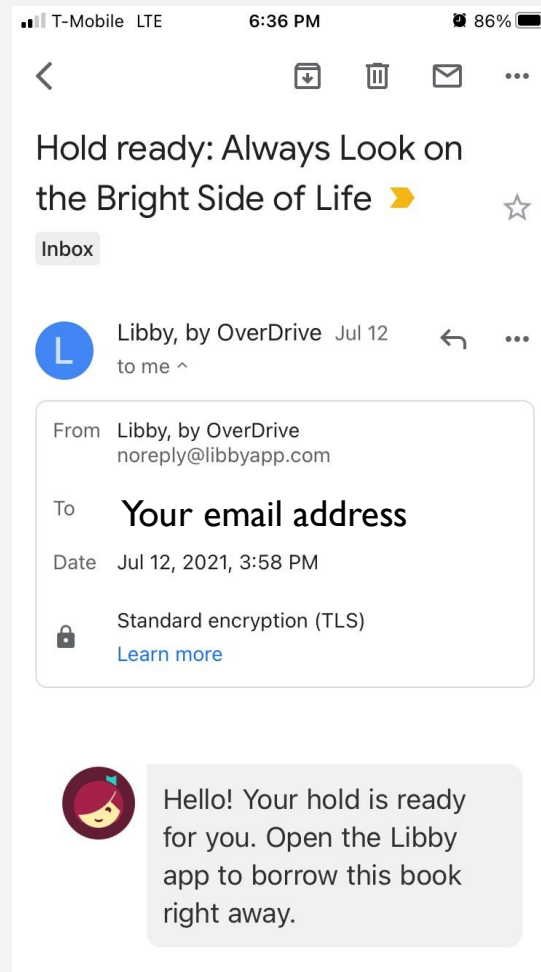
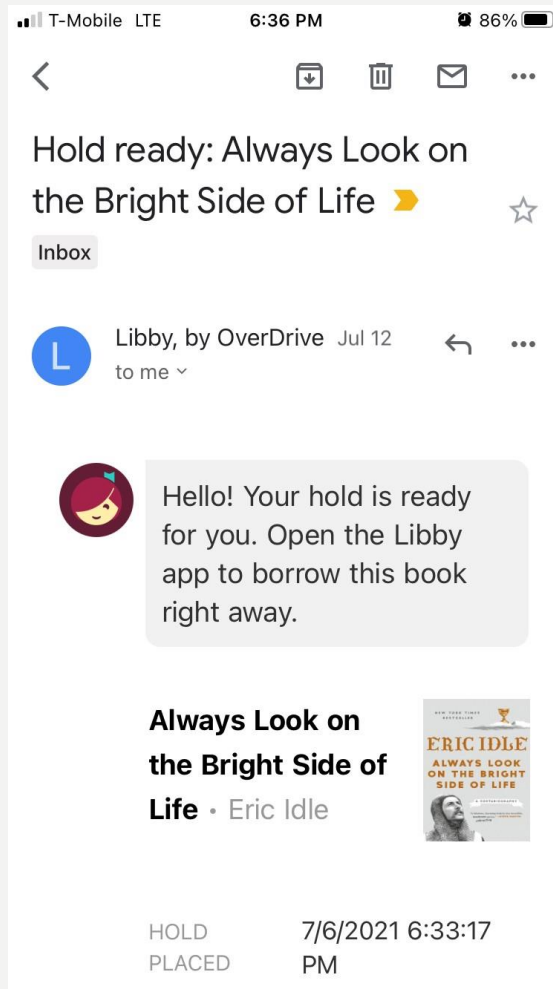
[Get Directions](#)

# EXAMPLE OF REAL LIBRARY EMAIL NOTIFICATION #1

- **Fresh News** – Broward County Library's official electronic newsletters that promotes library sponsored events and resources.



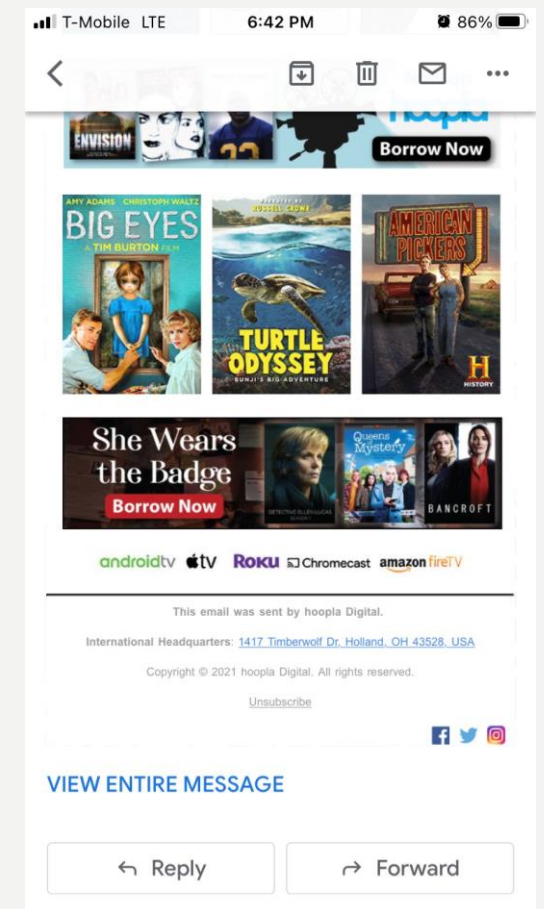
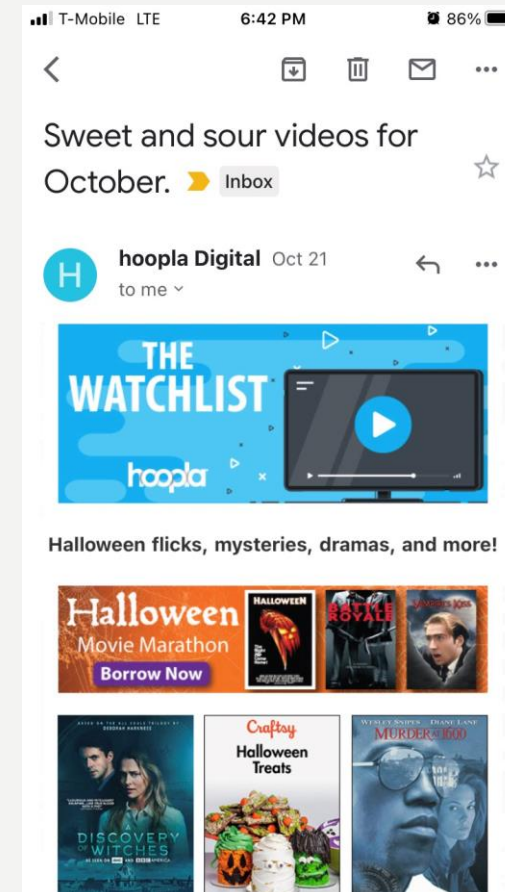
# EXAMPLE OF LIBRARY EBOOK EMAIL NOTIFICATION #2: LIBBY



# EXAMPLE OF LIBRARY EMEDIA EMAIL NOTIFICATION #3: HOOPLA

## Hoopla Digital is an eMedia app for all ages!

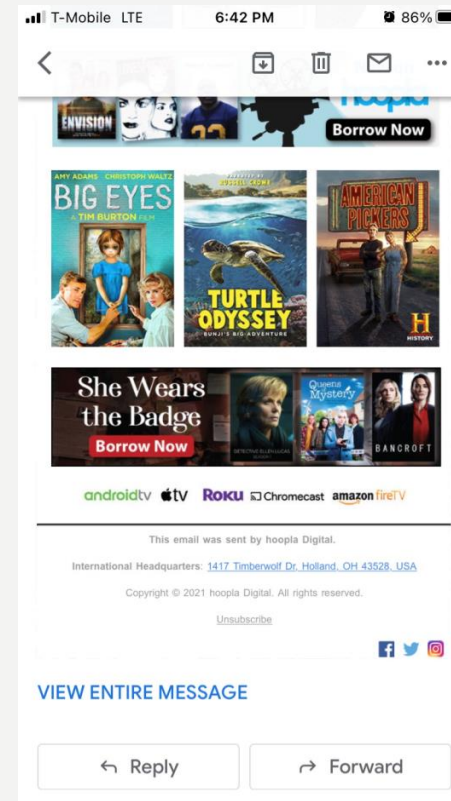
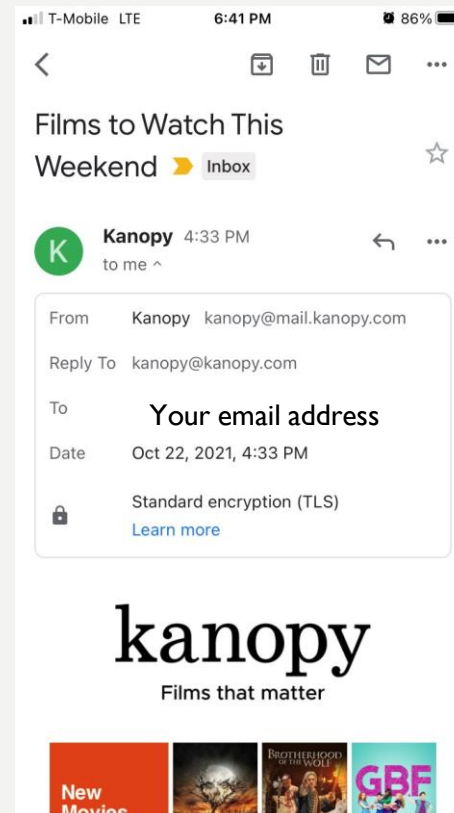
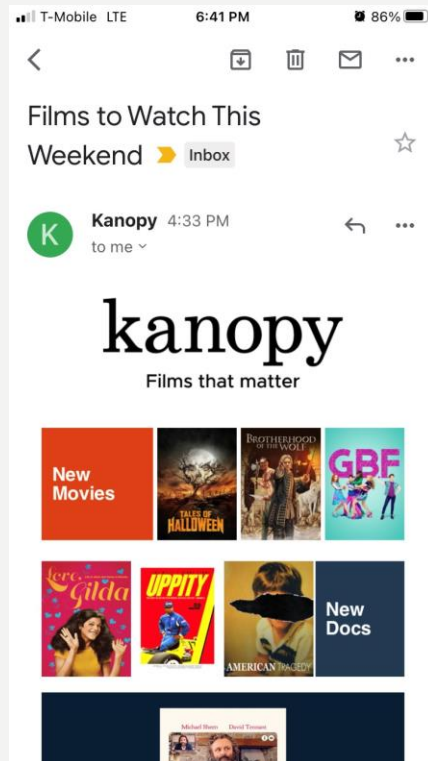
- Borrow 8 items per month with no wait lists.
- Inventory changes on the 1<sup>st</sup> of the month,
- eBooks, eAudiobooks, eComics (Graphic Novels): Borrow for 21 days.
- eMusic: Borrow for 14 days.
- Digital movies and television episodes: Borrow items for 3 days.





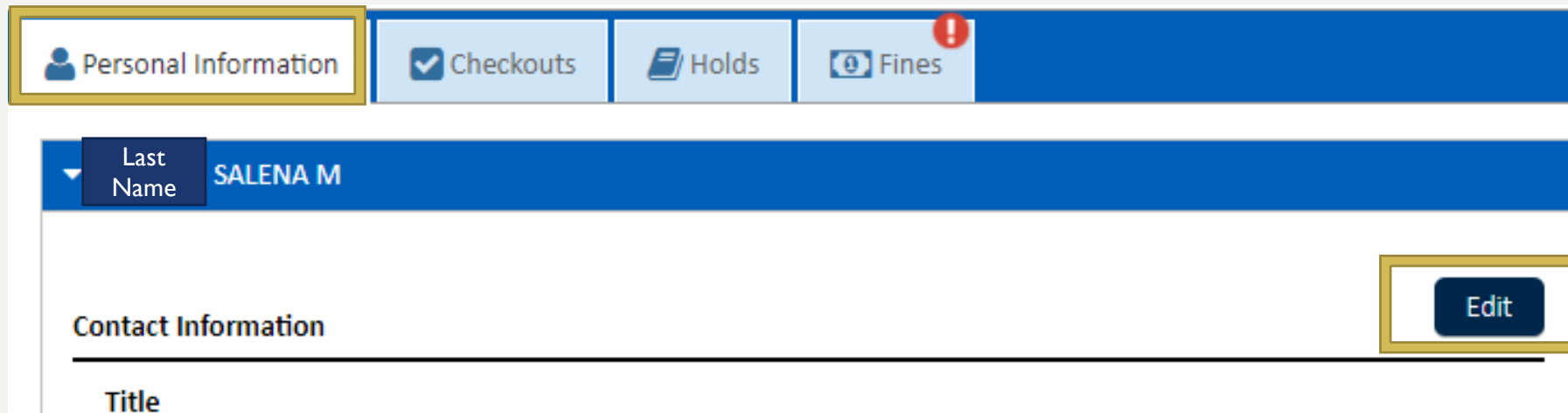
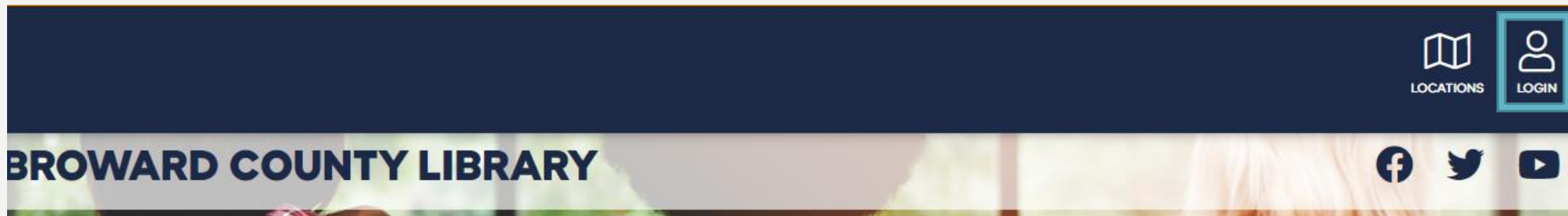
# EXAMPLE OF LIBRARY EMEDIA EMAIL NOTIFICATION #4: KANOPY

- Kanopy is an eMedia app for all ages!
- Borrow 6 titles per month (films or television episodes)



# CHANGE YOUR CONTACT PREFERENCES

- Log into your account [www.broward.org/library](http://www.broward.org/library) and select **Login**.
- Enter your library card and PIN numbers to access account.
- Select **Personal Information** and click on the **Edit** button.



# CHANGE CONTACT PREFERENCES

- Select the dropdown menu next to “**Notify By**”.

Language	ENGLISH
Library	MN
Gender	FEMALE
Notify By	<div>SMS</div>

FEMALE
<div>SMS</div>
EMAIL
PAPER
PHONE
SMS

# CHANGE CONTACT PREFERENCES

Address 3

Email

Fax

Mail stop

Office

Phone

Room

Type

Use for

Work phone

Save

Cancel

▶ Change PIN

▶ Preferences

▶ SMS Notifications



# WHAT TO DO IF YOU ARE SCAMMED

## FLORIDA'S IDENTITY THEFT VICTIM KIT

A GUIDE FOR VICTIMS OF IDENTITY  
THEFT, DETAILING WHAT  
TO DO AND WHO TO CONTACT.

1-877-IDTHEFT  
(1-877-438-4338)  
[www.Consumer.gov/  
IDTHEFT](http://www.Consumer.gov/IDTHEFT)

Visit the State of Florida's Office of Attorney General and download and read the online guide entitled ***Florida's Identity Theft Victim Kit:***

<http://myfloridalegal.com/pages.nsf/main/cbbeba3f2583433385256dba004bc600>

# WHAT TO DO IF YOU ARE SCAMMED

Contact the Federal Trade Commission:

[www.consumer.ftc.gov/features/scam-alerts](http://www.consumer.ftc.gov/features/scam-alerts)

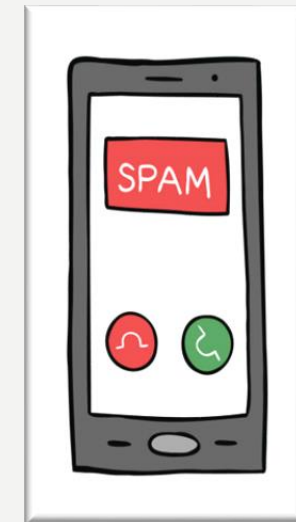


# COMMUNITY RESOURCE

- The ***Oasis Connections Guide to Online Safety*** created by the non-profit organization Oasis Connections: <https://connections.oasisnet.org/oasis-connections-guide-to-online-safety/>
- **Create Strong Passwords (a love/hate story):**  
<https://connections.oasisnet.org/oasis-connections-guide-to-online-safety/passwords-a-love-hate-story/>

# PASSWORD SECURITY: CREATING STRONG PASSWORDS

- Has 12 characters or more.
- Includes numbers, symbols, lower-case, and upper-case characters.
- Avoid any full dictionary words or names.
- Keep obvious substitutions to a minimum
- One piece of advice is to take a sentence you will remember and use the first or first two letters of every word, string them together and then add symbols and numbers.
  - An example is, “The first house I ever lived in was 613 Fake Street. Rent was \$400 per month.” That can be made into “Tfhleiw613FS.Rw\$4pm.” It is a sentence you may be able to remember and can create a unique word out of it. (Mental)
- **Source:** Mental Floss Editorial Staff. “8 Tips to Make Your Passwords as Strong as Possible.” Mental Floss. Retrieved from: [www.mentalfloss.com/article/504786/8-tips-make-your-passwords-strong-possible](http://www.mentalfloss.com/article/504786/8-tips-make-your-passwords-strong-possible) on 4/28/21



# PASSWORD SECURITY: ARTICLES WITH MORE INFORMATION

- Hoffman, Chris. "How to Create a Strong Password (And Remember It)." How2Geek. 5/9/2018.  
Retrieved from:  
[www.howtogeek.com/195430/how-to-create-a-strong-password-and-remember-it/](http://www.howtogeek.com/195430/how-to-create-a-strong-password-and-remember-it/)
- Hoffman, Chris. "Why you Should use a Password Manager, and How to Get Started." How2Geek. 7/10/2020. Retrieved from:  
[www.howtogeek.com/141500/why-you-should-use-a-password-manager-and-how-to-get-started/](http://www.howtogeek.com/141500/why-you-should-use-a-password-manager-and-how-to-get-started/)
- Reinhold, Arnold. *The Diceware Passphrase Homepage*. Updated 2/11/21. Retrieved from:  
<https://theworld.com/~reinhold/diceware.html>





# DATA PRIVACY

- National Cybersecurity Alliance (NCA) Resources and more about **Data Privacy Week**: <https://staysafeonline.org/data-privacy-week/about-dpw/>
- Manage Your Privacy Settings based upon what app, product, or service you are using: <https://staysafeonline.org/stay-safe-online/managing-your-privacy/manage-privacy-settings/>
- On your smartphone, make sure to delete unused apps and make sure to frequently update the apps you have installed.
- Manage your privacy settings on apps and social media. Limit what information you share about your current location, job, school, etc.
  - For example, on Facebook and other social media profiles do not add information about your home city, and your school or place of work.

# HOW TO PROTECT YOUR COMPUTER AND MOBILE DEVICES

- Make sure your Internet Browsing software is updated frequently.
  - Examples: Google Chrome, Mozilla Firefox, Safari (Apple), Microsoft Edge, etc.
  - Stop using [Microsoft Internet Explorer](#) and start using their newer software: **Microsoft Edge** with IE mode (enables backward compatibility and will be supported through at least 2029).
- Make sure your personal devices have current and active antivirus program like Windows Defender, Norton Antivirus, McAfee, Trend Micro, etc.
- Make sure your cellphone, tablet, or computer operating system is current and updated.
  - Examples: Microsoft Windows 10, or 11 Apple iOS, Android, etc.
- Protect your important personal files by backing it up on the cloud server or external hard drive.
  - Examples: Carbonite, Dropbox, Microsoft OneDrive, Google Drive, iCloud, etc.
- Protect Your Online Accounts with 2-Factor Authentication when it is available.



# LEARN MORE ABOUT NEW SCAMS WITH ONLINE NEWSPAPERS: SUN-SENTINEL, AND MORE

- Visit [www.Broward.org/library](http://www.Broward.org/library) and select **eMedia** from the menu.
- Scrolled down the page and under the **Newspapers** section select one of the newspapers: *Sun-Sentinel*, *NY Times*, *Wall Street Journal*, and *Washington Post*.
- If you need access to more local Florida newspapers like *Miami Herald*, *El Nuevo Herald*, then select *Sun-Sentinel* from the list and then select **A-Z Source List** from the **Newsbank** database and search by keyword.

## E-MEDIA

Your [Broward County Library card](#) offers you an amazing selection of free eContent that can be accessed from your computer and mobile devices.

**eBooks & eAudiobooks:** [Overdrive](#), [Axis 360](#) & more

**Music:** [Freegal](#), [Hoopla](#)\*

**Movies:** [Kanopy](#), [Hoopla](#)\*

**eMagazines:** [Overdrive](#), [Libby](#), [Flipster](#)\*\*

**Classes:** [Gale Courses](#), [The Great Courses](#), [Universal Class](#)

**Language Lessons:** [Rosetta Stone](#)

**Newspapers:** [Sun-Sentinel](#), [NY Times](#), [Wall Street Journal](#), [Washington Post](#)

Access World News | All Databases

**NewsBank** inc.

New Search

**A-Z Source List**

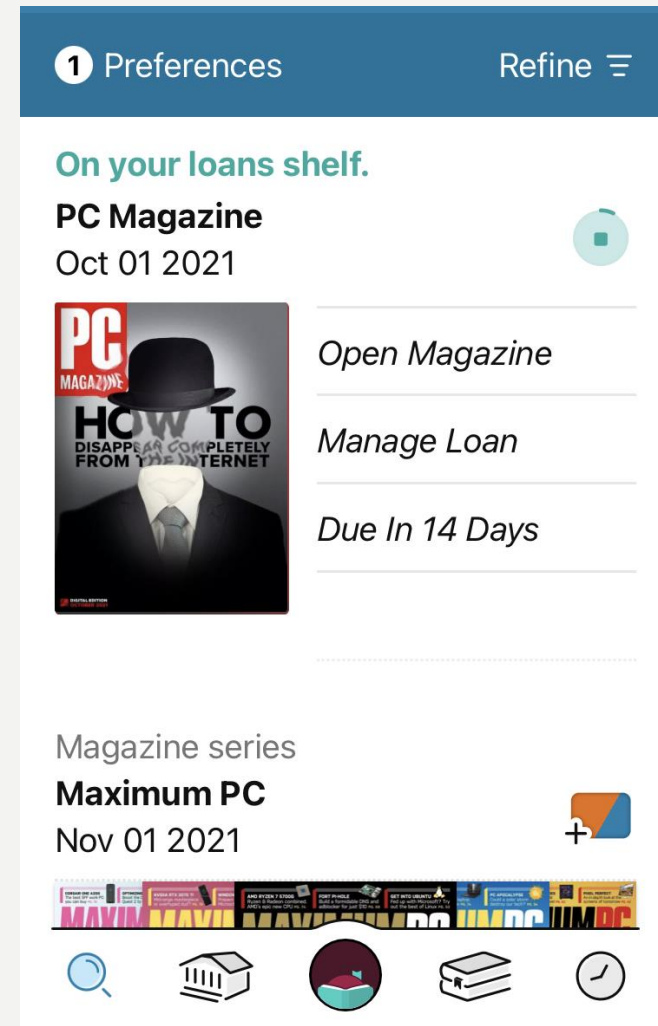
Session Folder ▼

## A-Z Source List

1 - 20 of 9,501 Sources

# LEARN MORE ABOUT NEW SCAMS WITH LIBBY'S E-MAGAZINES

- Access **PC Magazine** and other publications within the Libby app and you will find articles about new technology, Internet security and how to avoid new scams.
- The free Libby App works with these devices: Apple iOS 10 or higher (iPads or iPhones) and Android 5.0+ devices.
- Visit the Libby Help site for more information:  
<https://help.libbyapp.com/en-us/index.htm>
- If you have a Windows computer, Mac computer, or a Chromebook, you can use Libby in your web browser at [libbyapp.com](https://libbyapp.com). Libby suggests using the latest version of Chrome, Safari, Firefox, or Edge (Chromium).



# Q & A SESSION

- If you want the class notes or have additional questions, then please email: [scoller@broward.org](mailto:scoller@broward.org)
- If you have general library and reference questions, then please contact your local library branch for assistance. List of locations: [www.broward.org/Library/Pages/Locations.aspx](http://www.broward.org/Library/Pages/Locations.aspx)
- Presented by Salena Coller, Community Library Manager of the Galt Ocean Mile Reading Center and the Imperial Point Branch Library.
- Created by The Computer Center Employees working at the Broward County's Main Library.
- Updated September 2023