



Your identity. What Happened?

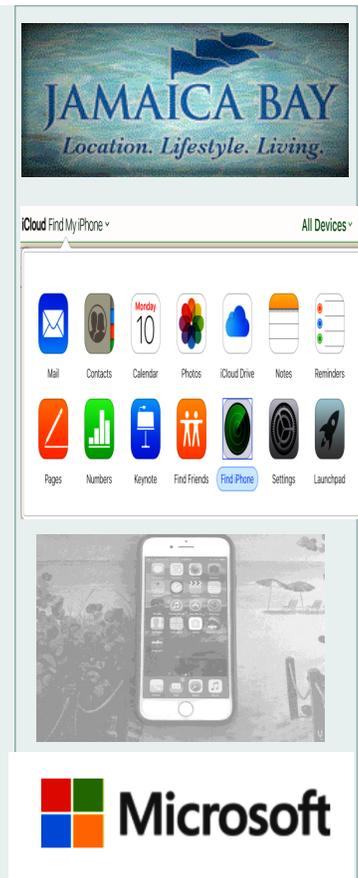
Part 1: an introduction to the Dark Web

The Dark Web is part of the internet that search engines, like Google, can't find. Because of that, sites in the Dark Web may be conducting illegal activity that may include your information.

Why should you care about understanding the Dark Web?

One primary reason is the type of illegal activity that can happen on the Dark Web is the trading or selling of personally identifying information. Thieves use these sites to sell or buy Social Security numbers, credit card numbers, email addresses, passwords, and other stolen or breached data.

What you can do? The first few steps are easy.
Continued on Page 2



INSIDE THIS ISSUE

The Dark Web	2
Basic Computer Edu	2
AARP & YOU	3
Bitcoin	4
Cryptocurrency	4
SSA protecting SSN	5
Create an SSA acct	6
Feb 2020 Jamaican	7
What's new at CES	7



WHAT THE EXPERTS SAY ABOUT KEEPING YOUR IDENTITY SAFE FROM THE DARK WEB.....

Make sure to create and regularly change strong passwords. *NEVER* use the same password on different sites!

Also, keep an eye on your financial statements for anything suspicious.

These are good practices, but they still may leave you in the dark when it comes to

specific threats.

Next, consider locking your credit. We talk about this at our club meetings all the time.

When surfing the net make sure your web browser points to "HTTPS:"

INSIDE STORY HEADLINE



All classes are taught by a trained Lee County school professional. Visit their website for the details

ADULT ADUCATION. WHAT'S NEW?

Lifelong Learning Classes

Adult Enrichment Courses for Every Interest. Affordable. Engaging. Fun!

Course Description: Computer Basics will make you a friend of technology. The class will cover the following:

- Operating computer (turning it on, etc.)
- Windows vs. Apple
- Logins and passwords
- Privacy/Safety/Spam
- File management (archiving, categorizing)
- Email (sending, saving, categorizing, attaching, etc.)
- Using social media
- Basic photo skills: where to save, how to attach, how to open
- Buying on the internet; how to be safe
- Don't get hacked!
- Connecting with other devices
- Saving files
- All materials are included in the cost of the class. Computers are provided.
- All Lee County Lifelong Learning classes must meet a minimum student enrollment or class will be delayed or canceled (if canceled, a full refund will be issued.)
- When registering, please use a current email that you check often in order to receive important class messages, date changes or cancellations.

Visit www.LEESCHOOLS.NET/LLC for more information. The cost for this particular class is \$53!



JANUARY 2020 WHAT AARP SAYS ABOUT FRAUD

Four Ways Fraudsters Like to Get Paid

A scam isn't complete until money has changed hands. So crooks expertly use all available methods to make that happen quickly and easily. Increasingly, they're using these four popular money-transfer approaches. Ask yourself, Would an ordinary business or government agency ask for money using one of these payment methods? If someone calls and seeks cash from you in one of these ways, take a long moment to consider.

MONEY-TRANSFER APPS

Peer-to-peer apps like Venmo, Zelle and Cash App allow you to move funds easily to a friend or relative who also has an account. But apps like these say in their user agreements that they are designed to be used by people who know and trust each other, and they note that they don't offer consumer protections. The best-known transfer app, PayPal, does mediate disputed transactions. But caution is critical when using most of these apps. If someone you don't know has something for sale and will take the money only via a peer-to-peer money-transfer app, you should decline.

WIRE-TRANSFER

These tried-and-true services are good for sending funds to loved ones. But criminals love them, too. Wire transfers are often requested as part of sweepstakes and lottery scams, where you are asked to send money to help process big winnings — which never materialize. When a MoneyGram or Western Union transfer falls into the hands of a crook, it's untraceable. There are limited protections on this type of transfer. If you are ever asked to pay for a product or service via money transfer, consider it a red flag.

CONTINUED ON PAGE 4

FRAUDSTERS RAMP UP THEIR SCHEMES IN THE NEW YEAR

Changes in Social Security cost-of-living benefits that went into effect Jan. 1 will open the window to a new round of scams, experts warn.

"The Social Security impostor scammers will use this as an opportunity to confuse you with messages about your accounts," says AARP Fraud Watch Network's Amy Nofziger. "Remember, the SSA will not call you to demand payment with prepaid gift cards or cash."

Those schemes rocketed to new highs in 2019. The Social Security Administration received more than 450,000 impostor complaints during the fiscal year ending Sept. 30, its Office of Inspector General says, up from 15,221 the previous year. Under this scam, criminals mislead victims into making cash or gift card payments or wiring money to avoid a phony threat to shut down their Social Security account.

From AARP online at <https://www.aarp.org/money/scams-fraud/info-2020/how-scammers-get-paid.html>

(Edited by Carl Blasé)

INSIDE STORY HEADLINE

BITCOINS: The Cryptocurrency scammers and identity thieves what. It's the primary currency used in the DARK WEB.

It's practically untraceable when exchanged between two parties.

It's completely legal. All financial markets around the world follow and invest in BITCOINS and the underlying technology behind them.

You've probably heard the term **BLOCKCHAIN**. This is the technology that allows BITCOINS to be traded.

To learn more, search the internet for these 2 terms and you'll find a ton of information.

OR go to the computer club website

jamaicabaycomputerclub.com and search for Bitcoin or read my series of articles on the Dark Web



.....CONTINUED FROM PREVIOUS PAGE

AARP— WAYS FRAUDSTERS GET PAID

STORE GIFT CARDS

As we have previously reported, gift cards have become a favorite way for scammers to cheat you. One common con: You get a call from a person alleging to be an IRS official who says that you owe back taxes. Or you are called about an unpaid traffic ticket from someone claiming to be a lo-

cal police officer. The person requests payment via gift card from a major retail chain. You are directed to buy the cards for up to several hundred dollars, then read the code numbers on the back of the cards to the caller. Once you've done that, the swindler can use the codes to buy merchandise — including other gift cards with lower denominations. That makes the cash untraceable.

Cryptocurrency

The AARP Fraud Watch Network helpline has gotten calls from more than 80 people in the past two years who encountered crooks requesting cryptocurrencies like Bitcoin. While not as common as some other forms of payment preferred by con artists, their use is growing. The Federal Trade Commission recently reported that these virtual currencies were being requested in the Social Security scam, in which people are falsely told a payment is needed to unfreeze an account. Victims are instructed on how to open an account and told to buy a fraction of a Bitcoin, for example, in increments of as little as \$10. Transactions take a few minutes and are person-to-person, without any bank or regulating body. When the crook gets your money, it's gone.

So, how should you pay bills or shop online? We recommend using a credit card for most transactions, as they have added protections that other forms of payments don't. As for these other means of making transactions: Use them only with people you know and trust. Paying someone you've met online with these types of currency is always risky. Don't help crooks use these popular fund transfers to perpetuate their scams.

PROTECTING YOUR SOCIAL SECURITY NUMBER

Social Security maintains a robust cyber-security system, but you are the most important factor in helping us keep your information safe. You can help by:

- **Opening your personal my Social Security account.** Create your account today and take away the risk of someone else trying to create one in your name, even if they obtain your Social Security number
- **Add a second method of identification to your my Social Security account.** If you already have a my Social Security account, but haven't signed in lately, take a moment to log in to easily take advantage of our second method to identify you each time you log in. This is in addition to our first layer of security, which is a username and password. You can choose to use either your cell phone number or your email address as your second identification method. Using two ways to identify you when you sign in will help protect your account from unauthorized use and potential identity theft. If you suspect identity theft, report it to our Office of the Inspector General and visit www.identitytheft.gov.
- **Other ways to protect your information include not routinely carrying your card or other documents that display your number with you.** Also, be careful about sharing your number, even when you're asked for it. You should ask why your number is needed, how it'll be used, and what will happen if you refuse.
- **Sign Up for an Optional Extra Level of Protection** You can opt for an extra level of protection for a my Social Security account. Individuals seeking this extra security must answer a financial verification question.
- **Sign up for extra security at registration.** When you first register for a my Social Security account, you must verify your identity by answering an additional security question. We'll ask for one of the following: — the last 8 digits of your Visa, MasterCard or Discover Card; or — information found in your W-2 tax form; or — information from your 1040 Schedule SE (self-employment) tax form.
- **Signing up for extra security if already have a my Social Security account.** After logging in to my Social Security, go into the "Security Settings" tab to begin the upgrade process. "Add Extra Security" is the first option in the Security Settings tab. Follow the instructions to add the extra security to your authentication process. Finishing this process usually takes 5 to 10 business days. An upgrade code will be mailed to your home address. The letter will also include step-by-step instructions to finalize the security upgrade.



Social Security

Block Electronic Access If you know your Social Security information has been compromised you can use our Block Electronic Access.

You can block any automated telephone and electronic access to your Social Security record. No one, including you, will be able to see or change your personal information on the internet or through our automated telephone service.

If you block access to your record and then change your mind in the future, you can contact Social Security and ask us to unblock it after you prove your identity.

How to create a *my* Social Security account



Securing today and tomorrow

To create an account, you must:

18

Be at least 18 years of age



Have a Social Security number



Have a valid U.S. mailing address



Have an email address

START HERE

1

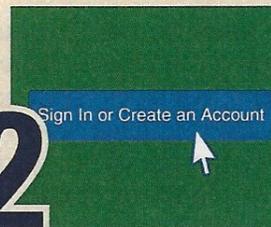
Visit

www.SocialSecurity.gov/myaccount



2

Select



3

Select



7

Create account detail



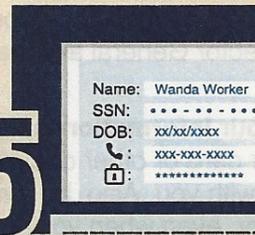
6

Verify your identity



5

Tell us who you are



4

Read and agree to our Terms of Service



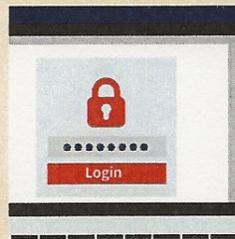
8

Select how to receive your security code



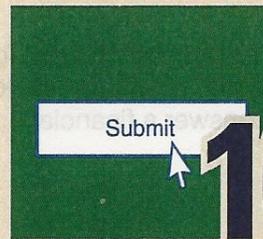
9

Enter the security code you received

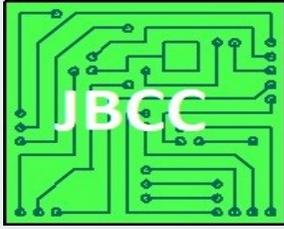


10

Send and congratulations, you successfully created an account!



Create Your Account Today!



www.jamaicabaycomputerclub.com

jamaicabay-computeclub@gmail.com

New Product from CES 2020

The new Oral B IO connected smart toothbrush is taking brushing up a level. Connected to an app over Bluetooth, the brush is able to show your progress brushing and track the different areas of your mouth that you've brushed.

It has a status light on the neck that glows green when you apply the right amount of pressure and red if you apply too much.

A display on the brush lets you know how well you brushed post brushing session. That is also where you can change the brushing mode, language, or LED colors.

Club article for Feburary 2020 Jamaican

Official start time is 1:30 but come early to meet and ask questions. We setup at 12:30 and close up at 3pm.

Darn it. I keep writing 2019 on my checks and receipts. (does anyone actually say "darn it" anymore?)

At our last club meeting for 2019, for an hour & 15 minutes Kris from Computer Medics did a great job explaining Apple core apps such as setting up Mail and calendars. He showed differences in the iPad, iPhone & Mac laptop.

Did you get a new mobile device such as an iPad, iPhone or laptop for Christmas? Bring it to a club meeting. At our December 23rd, all of our members had iPads or iPhones. Don't pass up an opportunity to meet a neighbor who might be able to help you!

If you are just now reading this, you've missed the final Computer Medics presentation in January. Kris once again focused on Apple applications and devices in more detail. If you did not come to any of Computer Medics four presentations because of the "P" word (procrastination) or if the timing was just not right, well, there's always next year.

We'll still be discussing Apple & mobile devices at our meetings but now the emphasis will be on Microsoft Windows 10.

* **Important notification** *

We are having a Special presentation by Lee County Sheriff's department. **I'm asking for your support at the second club meeting in February.** This will be the 19th. You DO NOT have to be a computer user or club member to benefit from this discussion about fraud against seniors and how the "dark web" is used to buy & sell your identity, your credit cards, or your email if stolen.

At our first meeting in February, the 5th, we will spend some time looking at Chromebooks. We will also provide a list of keyboard shortcut commands. Does your computer run "slow?" We will be discussing why this might be happening and what you could do about it. In preparation for our special meeting by the Sheriff (see previous paragraph) we are going to talk about the DARKWEB. If you want a head start there is a 3 part article on the club website. Go to this link: <https://www.jamaicabaycomputerclub.com/darkweb-1>

From your club co-leaders

Gary 887-0585 gary.torrez@ymail.com

Chuck 817-2816040 black118336@gmail.com

Official start time is 1:30 but come early to meet and ask questions. We setup at 12:30 and close up at 3pm.