FAULKNER UNIVERSITY

Phillip Calvert <pcalvert@faulkner.edu>

Monthly News and Commentary from ICJE

1 message

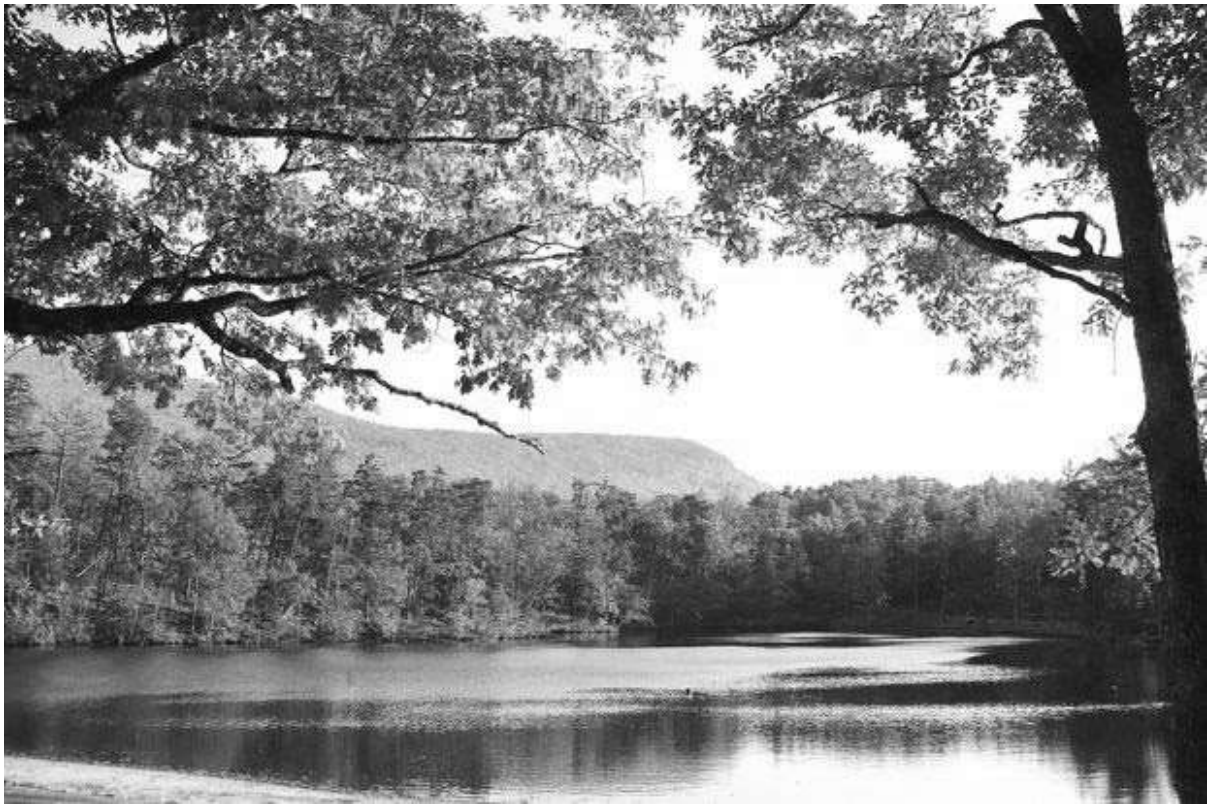
ICJE, Inc. <jimrechel@icje.org>
Reply-To: jimrechel@icje.org
To: pcalvert@faulkner.edu

Fri, Sep 16, 2022 at 10:51 AM

August/September 2022

INSTITUTE FOR CRIMINAL JUSTICE EDUCATION

Summer's Swan Song



A slowly falling leaf, with the golden glow of a coming fall season, let's go of its perch from which it surveilled summers' fun, and flutters to the ground, announcing the ultimate end of summer.

Summer's end is subtle, sneaking in through the backdoor, under the cover of a late summer cicada's call. The reach of the live oak's shadow, and garland of Spanish Moss beckons us to seek relief from the September heat, while suddenly, without notice, the vines on the fence turn golden orange, and the corn stalks yield their green to shades of brown. The tassels turn brown, and join with the sunflowers, as they collectively bow down, choreographed by God's hand, whispering that summer's end is near.

Baseball fields stand eerily quiet, except for an occasional "dust tornado" stirred by the afternoon winds. The empty benches, and chain link backstops seem to be asking "Where is everyone? Are you coming back?"

The lifeguard at the local pool oversees but a handful of kids, whose schools start later than the rest of their friends. Splashing about, they squeeze as much summer as possible into their lives before they too must join the army of yellow buses, carrying book-bags heavy enough for "the Army".

But just as the days grow shorter, and the night's cooler, the beauty of a new season is announced. The beauty of falls' glorious color is just around the corner. The quiet stillness of an early fall night is pierced by the cheers from the stands of a Friday night football clash or Saturday afternoon college clash.

On God's field it is Summer vs. Autumn, and in this clash both teams will win, for God's glory is in every season.

May God bless you.

Jim Rechel,
ICJE Newsletter Editor
jimrechel@icje.org

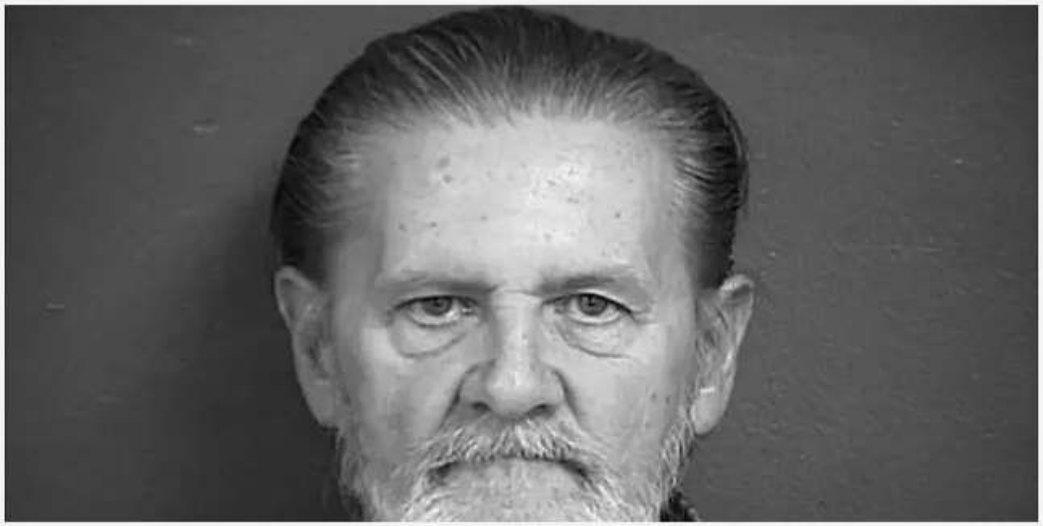
Please feel free to email comments or suggestions. Thanks, Jim

Hmmm...

I came upon this headline while researching Kansas bank robbery stories for training I'm doing there in a couple of weeks.

As we often complain about lenient sentences for crooks, I think this judge's sentence could be the harshest sentence the defendant could receive! Read on to better understand....

Kansas man who robbed bank to escape wife gets home-confinement sentence



NEWYou can now listen to Fox News articles!

A Kansas man who robbed a bank last September and told police that he was hoping to get caught so he would get prison time to escape his wife, was sentenced Tuesday to six months of home confinement after pleading guilty, The Kansas City Star reported.

LECC 2022 Conference - 32 Years and Running

Orange Beach was awash with law enforcement, as more than 300 attendees were provided to outstanding accommodations and fantastic speakers and topics on a variety of issues impacting law enforcement and our society in general. Of particular interest to attendees were presentations on gangs, guns, cell data analysis, cybercrime, investigations and establishing the culture for organizations. It was a pleasure to be part of another great conference.

Thank you to all who made it happen, especially Doug Howard and the team in the US Attorney's office throughout the state.

Phone Porting and Keeping Passwords on Your PC

For small businesses and individuals, beware of computer breaches and phone porting. Two family businesses I'm familiar with recently lost more than $400,000.00!

A personal computer was apparently accessed by bad guys, and in the files, they found an Excel spreadsheet the business owner had created which contained usernames and passwords to hundreds of websites. The bad guys most likely gained access by duping the user into clicking a malicious link, or other similar technique.

They then used the information to port the owners cell phone number to a new phone, then requested wire transfers.

Among other verifications, the bank called the phone number in their files to verify the wire request. Little did anyone know, but the call was forwarded as a result of the fraudulent port to a phone the bad guys controlled.

For those of you who use a cell phone as the primary number used with your financial institution, take the additional steps to secure your phone and the ability to defend against fraudulent porting.

How Do I Protect Myself from Port-out Scams?

Courtesy: NordPass.com

Once bitten, twice shy – if you've been a victim before, you're going to make every attempt and precaution available not to let it happen again. As with all kinds of fraudulent behavior, the best way to prevent such things happening is to educate yourself.

Here's what you can do to reinforce your security against phone porting:

- Get a password manager. The best way to prevent anyone from guessing your password? An encrypted app that will automatically create and store jumbled, cryptic passwords – alongside auto-filling in the required fields when needed, so you don't need to remember them. NordPass is the perfect addition to your arsenal.

- Apply a security PIN to every account that will allow it. A code that you'll have to enter before any changes can be applied. Whether it's changing your service provider or SIM card, no one will be able to do anything without this code. Don't make this PIN an obvious number – make it a unique combination you've never used before.

- Be wary of any 'do-this-now-to-save-your-account' messages. Take notice of the language of the message – it's trying to bait you into doing something rash. Ever had a pop-up on your computer that flashes red and tells you that your desktop is suddenly infected with a virus? It's the same concept, so don't fall for these fear tactics. Banks or phone service providers will never use that kind of loaded language.

- Take advantage of what's readily available to you. Banks will offer a plethora of security options to strengthen your digital defenses. Try to avoid using SMS OTPs – instead, opt for two-factor authentication. All banks now provide alerts straight to your email that will warn you of any suspicious behavior on your account. Make sure you turn that feature on. All these security additions will take less than 5 minutes to set up, and it can save you hours worth of grief.

- Call your bank or service provider. All these companies will have a customer service helpline. If you're questioning potential suspicious conduct, then call them up and inquire about the most recent activity on your account.

Simple Text Message Started It

On September 16, 2022 an individual claiming to be behind the security breach at Uber told The New York Times that they had simply sent a text message to an Uber worker pretending to be a corporate IT person and were promptly provided with a password that allowed them to gain wide-reaching access to Uber's systems.

Rachel Tobac, the CEO of SocialProof Security, which helps train firm's on how to defend against cyber criminals, **wrote on Twitter** that there has been a major increase in SMS phishing of late.

SMS phishing is one of the many methods used by scam artists to lure people into handing over their personal or financial information via text message or other mobile messaging services like WhatsApp.

> "The person who claimed they just hacked Uber is saying their method was: – Send SMS phish to Uber worker as IT Support –

Steal credentials – Access Slack & internal systems," Tobac wrote.

The expert hacker added that there has been a rise in SMS-based phishing because it's "working" and "becoming increasingly well documented by attackers, and there are now kits that make it easier to develop attacks to steal passwords and MFA codes."

She added that a Fast Identity Online (FIDO) key, which uses things like fingerprint login and two-factor login to identify users, likely would have helped to prevent Uber's latest incident.

Phishing Scam Dupes Uber Employee

FCC Considering Proposals to Fight Port Out Fraud - From TheVerge.com

The Federal Communications Commission (FCC) on Thursday said it's looking into tightening rules around cell phone service, in an effort to rein in SIM swapping scams and port-out fraud, two ways fraudsters can access a person's cell phone account and phone number for nefarious purposes.

The agency says in a statement it has received numerous complaints "from consumers who have suffered significant distress, inconvenience, and financial harm" due to SIM swapping and port-out fraud. And, the FCC said, recent data breaches have exposed customer information that could make it easier for bad actors to carry out these kinds of attacks successfully.

SIM swapping is when someone hijacks your cell phone number so they can intercept two-factor authentication codes — the ones you use to verify a log-in or account access — to gain access to your account information. Typically, a bad actor is able to convince their victim's cell phone carrier to transfer service to a different device, which the victim doesn't have access to, but the bad actor does.
Port-out fraud happens when the fraudster poses as their victim and opens an account with a different cell phone carrier than the victim's and has the victim's phone number transferred — or "ported out" — to the new account with the different carrier.

In most instances, if the bad actor has access to a piece of personal identifying information, they can pull off either (or both) of these scams before the victim realizes what has happened.

Most security experts recommend using a third-party authenticator app to provide 2FA rather than receiving a text message with a log-in code, which is a less secure method.

The FCC has now issued a formal notice of proposed rulemaking and said in a **press release** it wants to amend the current rules to require carriers to adopt more secure methods of authenticating a customer's identity before they redirect service or a phone number to a new device or carrier. The agency is also proposing requiring carriers to immediately notify a customer whenever a SIM change or port request is made on their account.

Information Below from previous ICJE Newsletter in light of massive increase in Phishing Attacks

Staying Safe in an Unsafe World

The Triple-A Plan: Action – Protection from Internet Fraud and Cyberattacks

Internet and Other Fraud Schemes

As if things weren't bad enough with everyday cyber-criminals, now we know that the same cyberattacks that Russians are using against Ukraine can just as easily be switched to the U.S. with much greater effect. Our increased vulnerability is due to our dependency on the Internet for everything from the electrical grid to financial, water, and transportation systems, not to mention our personal computer systems.

The suggestions provided below apply to any online attack, and while there are no guarantees that your system will be safe, you will be protected to a much greater extent than those who have little or no safeguards in place. To give you some idea about the magnitude of fraud schemes today, the FBI's Internet Crime Complaint Center (IC3) provided a report in 2020 showing the following reported complaints in the U.S. where Elders were listed as victims:**[1]**

[1] https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3ElderFraudReport.pdf

- The scammer requests payment via gift cards, wire transfers, or virtual currency.
- The scammer creates a sense of urgency or deadline to pay quickly.
- The scammer demands secrecy from you.
- The contact contains poor grammar or misspellings.
- Payments are offered in amounts higher than a listed or normal price.
- Email addresses disguised to seem legitimate.
- Unsolicited emails, texts, etc., requesting you confirm usernames and/or passwords.
- Requests to move to a new platform to communicate.
- Requests to access your personal bank or other accounts to pay you for a service.

- Unsolicited emails with links or attachments.

Vital Defensive Measures

Because we can't always recognize the contact as fraudulent, there are a few defensive measures that can assist in keeping our identity and information private and safe.

1. Use a Virtual Private Network (VPN). A VPN will hide your identity and location, making it much more difficult for scammers to obtain your personal information, particularly in open access areas like hotels, airports, and restaurants. Without a VPN, it's as if you are inviting the bad guys into your home. Avoid the free VPNs as they don't normally offer the same protection as the paid services provide. Recommended VPNs are Express VPN, Private Internet Access, and Hideaway VPN.

2. Use a Password Manager. The password manager securely stores your passwords so you don't have to remember them. Password managers provide very strong passwords for all of your secure online sites and should be used by anyone linking to any financial or commercial site. A couple of the most popular are Dashlane and Roboform. These are easy to use and highly recommended.

3. Use Two-Factor Identification (2FA) whenever possible. 2FA adds an extra layer of security to your accounts by adding an additional step between putting in your password and accessing your account. This additional step is added to the log-in process and usually consists of a code sent to your phone or email or a fingerprint scan before accessing your account. It's like providing your PIN number before being allowed to access your ATM account. You may have the card, but without entering the PIN, no cash can be disbursed.

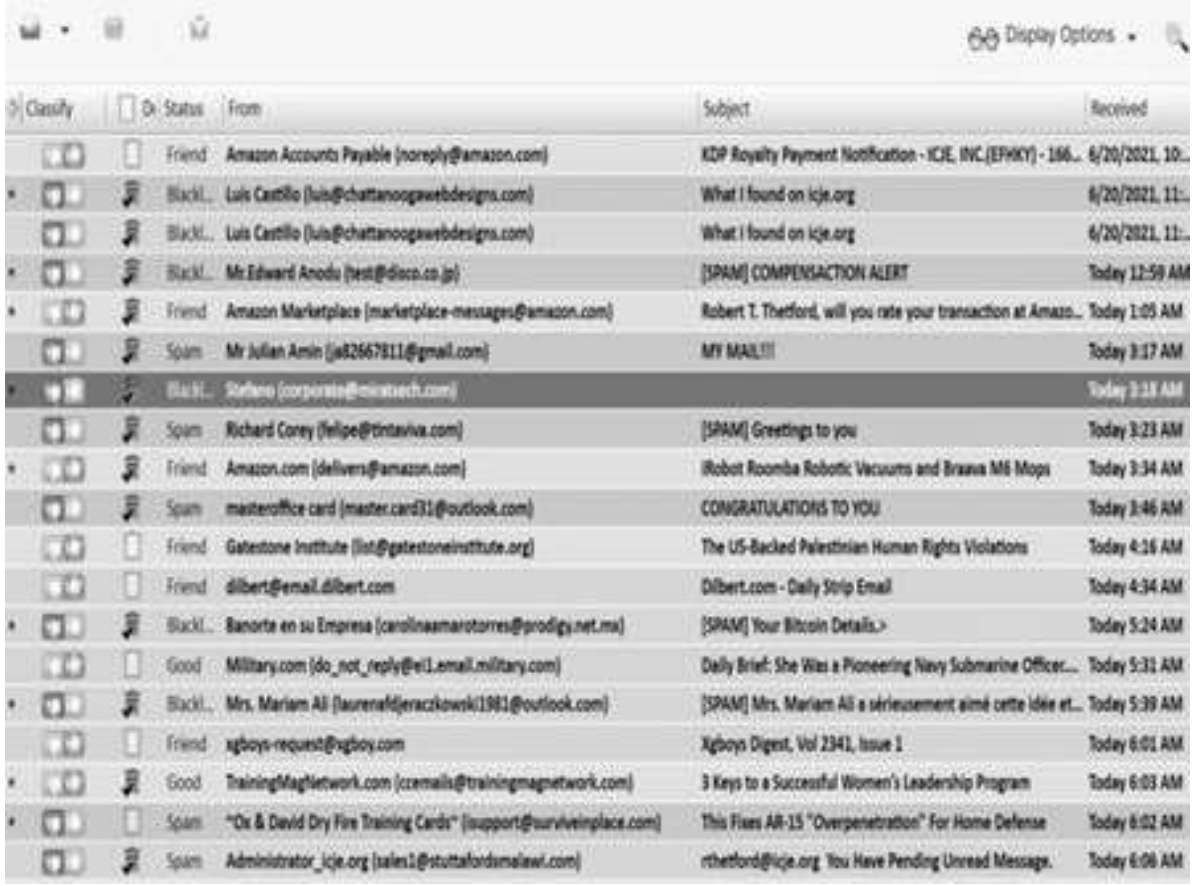
4. Also, make sure you have an anti-virus (AV) program. There are many free AV programs, but like the old saying, "There's no such thing as a free lunch," many of these programs collect and sell your personal information. For this reason, paid programs like Norton, Webroot, or Bitdefender are generally considered much better. Some programs, like Norton, offer security suites that include VPN and password managers in addition to the AV feature.

5. Back up your files frequently either through an external hard drive or an online service. Backing up your system offers protection from both equipment failure and ransomware attacks.

6. Finally, for those of you who are paranoid (and you should be), consider using an identity theft service like LifeLock or Identity Guard. They are not cheap, but with the increasing number of cyber-attacks, these programs have moved from the luxury class to the necessary class. The last time I checked, Identity Guard was a little cheaper than LifeLock for the same level of service.

7. Another highly recommended program to protect against email Spam or Phishing attacks is Mailwasher (**www.mailwasher.net**). Mailwasher is a program that reviews all of your incoming email messages and flags those that it recognizes as spam or malware. You can also review the message and sender, and if they look suspicious, you can mark them as spam, and they will be automatically deleted before they reach your email inbox. Mailwasher has a free version. If you find the program useful, keep the free version, or for more options, use the paid version.

- Below is a sample of the Mailwasher incoming emails. Note the red email headers (flagged as spam) vs. the green headers (friends). If you get a lot of emails, particularly spam emails, this is a great program to have.



Sample Threat Emails

Below are some sample threat emails that are obvious (and not so obvious) attempts to have the recipient respond or click a link. Either response may ultimately lead to accessing your system, including your financial records.

Beware of anyone offering to give you something for free.

From: Andrew Bailey
Sent: Wednesday, April 28, 2021 4:44 AM
To: rthetford@icje.org
Subject: [Norton AntiSpam][SPAM] INHERITANCE CLAIMS!!!! 58.215.166.242

Follow Up Flag: Follow up
Flag Status: Flagged

Hello,

Hope you are having a good day and the Covid-19 is not hitting hard on your side. I would like to know if you got my previous email with regards to the inheritance claims I informed you about earlier. Please let me know your interest. I will send further details if you wish to proceed.

Best regards,
Andrew Bailey

Beware of any email sent from a foreign country.

From: Lee Young <powerball@saocarlos.sp.gov.br>
Sent: Tuesday, April 27, 2021 4:09 AM
To: undisclosed-recipients:
Subject: [Norton AntiSpam][SPAM] Ref #: EAAL/851OYH1/15

Brazil

Follow Up Flag: Follow up
Flag Status: Flagged

Dear Beneficiary,

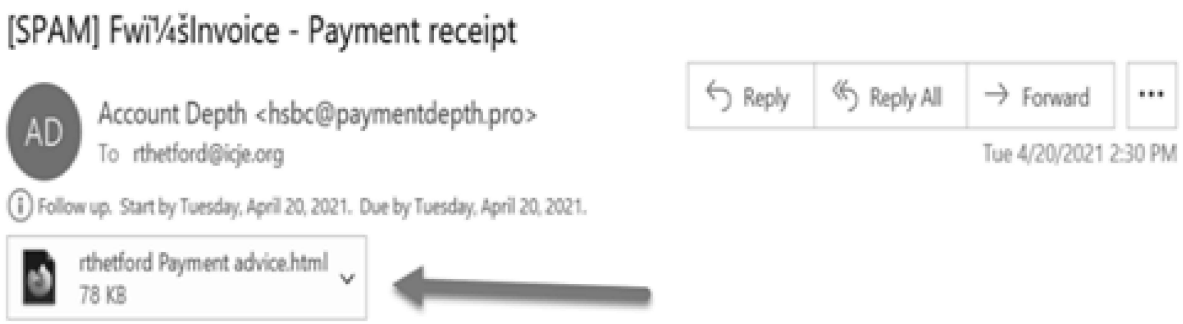
Your email was selected in Powerball Online Lottery Promo 2021 Draw with the sum of $350,000.00 USD.

Kindly the complete details for your claims.

Name:
Address:
Mobile Number:
Home/Alternative Phone Number:
Age:
Occupation:
Nationality:
Country of Residence:

Yours Sincerely,
Lee Young
Notification Officer (Sec. Zonal Co-coordinator)

Beware of opening any email attachment from an unknown source.

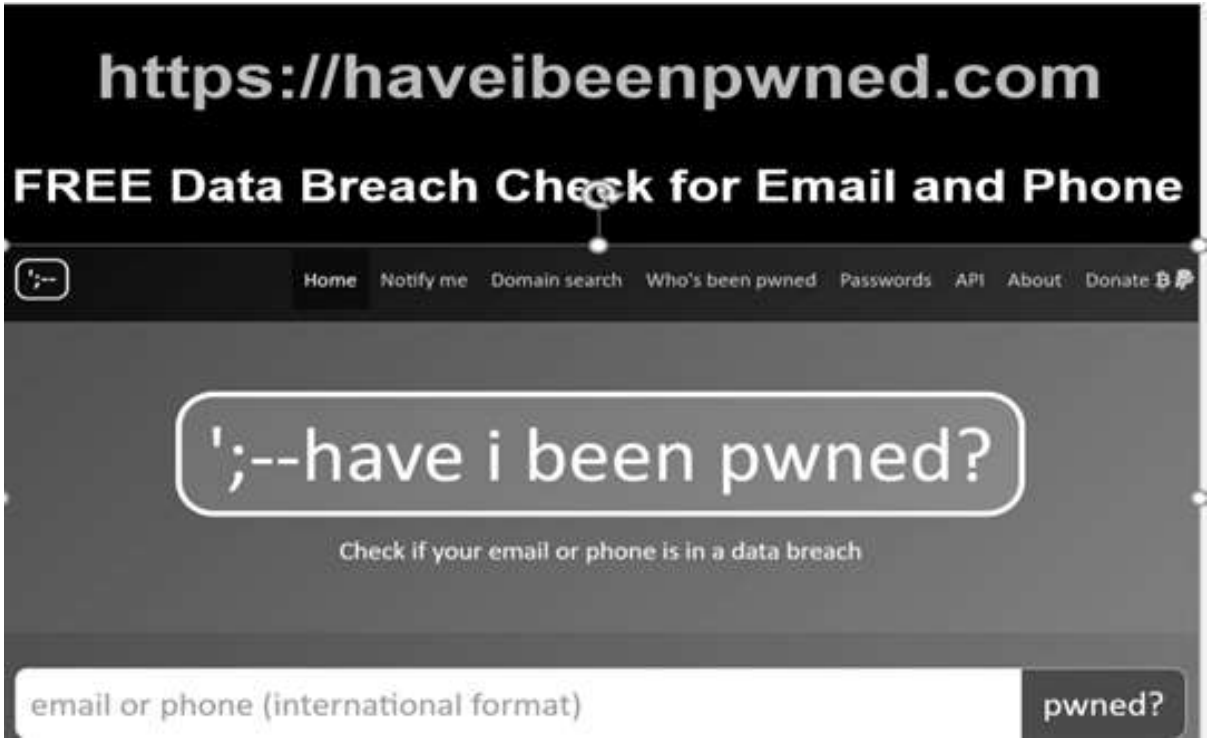


rthetford,

PAID
Tuesday, April 20, 2021 9:30 p.m.

rthetford@icje.org

Finally, it's not a bad idea to check and see if your email or accounts appear on the "dark web," meaning websites that traffic in stolen email, financial and other private information. Here is the link to the "Have I Been Pwned" website, a legitimate free service that keeps track of stolen identity information and allows you to see if your information is available to others. Pwned is gamer talk for "owned," so if you have been pwned, someone "owns" you. (**https://haveibeenpwned.com**)



Hopefully, these tips will help keep you safe from some of the online threats in today's world. **Summary: There are no guarantees that your computer system will be protected against cyberattacks, but there are specific steps you can take to avoid attacks. These steps include using a Virtual Private Network, Password Manager, Two Factor ID, and an Anti-Virus program. Don't forget to back up your files frequently and closely examine emails before opening them.**

This concludes our Staying Safe series. I hope you gained some tips to keep you and your family safe during these increasingly troubling times. Please let us know if you have any questions or tips.

For comments or suggestions, please get in touch with us at **training@icje.org**.
Thanks, and stay vigilant.

Bob Thetford
ICJE, Inc.

Training Information from ICJE Website

Visit the ICJE Website

September 26-30, 2022 - FBI LEEDA Media and Public Relations - Decautur, Alabama
More Information and Registration

October 27, 2022 - 2022 Alabama Attorney General's Law Enforcement Summit - Montgomery, Alabama
More Information and Registration

October 31 - November 4 - Southeastern Leadership Executive Development Seminar - Opelika, Alabama
More Information and Registration

November 14-18, 2022 - FBI LEEDA Command Leadership Institute - Fultondale, Alabama
More Information and Registration

January 9-13, 2023 - FBI LEEDA Supervisor Leadership Institute - Columbiana, Alabama
More Information and Registration

February 27-March 3, 2023 - FBI LEEDA Executive Leadership Institute - Fultondale, Alabama
More Information and Registration

March 13-17, 2023 - FBI LEEDA Command Leadership Institute - Columbiana, Alabama
More Information and Registration

May 15-19, 2023 - FBI LEEDA Executive Leadership Institute - Columbiana, Alabama
More Information and Registration

Other Training Opportunities:

AUM Continuing Education and Community Engagement

FEMA Emergency Management Institute

APOST Law Enforcement Training Academy - Tuscaloosa

Jefferson County Sheriff's Department Training Center

Northeast Alabama Law Enforcement Academy

Ozark Police Department Training Division

University of North Alabama Public Safety Institute

Link to Visit the ICJE Website for Registration and More Dates

Additional Resources

IAFCI - The PROTECTORS Podcast

About the Podcast

Presented by the IAFCI

From ATM Skimming to Human Trafficking, The Protectors Podcast takes you inside the minds of criminals from around the world with leading
experts and the investigators who put them behind bars.

Presented by the International
Association of Financial Crimes Investigators (IAFCI), and hosted by International President,
Mike Carroll, and International VP, Mark Solomon.

The Protectors is a bi-weekly podcast that aims to educate consumers on the fraud, financial,
and cybercriminal activities that are happening every second of every day. Don't become the next victim.

Link to Podcasts

Thought of the Month

“A nation cannot long remain strong when every person belonging to it is individually weak”

— Alexis de Tocqueville, Democracy in America