



VRSA

Virginia Risk Sharing Association

Cybersecurity: Let's be Cyber- Smart

Presented by: Thomas Bullock,
Director of Education and
Training

The Cyber Monster



2



- “If it is predictable, then it is preventable.”

❖ Gordon Graham



Cybersecurity Is Not Just an IT Issue...

Cybersecurity



4

- Cybersecurity is first and foremost a people problem rather than a technology problem;
- Increasing cybersecurity literacy and teaching people the basics of how to behave securely online;
- Will have compounding effects in reducing risk and in lowering the impact of any incidents.

The “Scary” Truth: Phishing Cyberattacks



5

- According to IBM’s Cost of Data Breach Report, phishing is the costliest type of cyberattack in 2022, costing \$4.91M;
- Human error is (still) consistently the leading cause of cybersecurity breaches, accounting for 95% of all data breaches;

How to Identify Phishing Scams



6

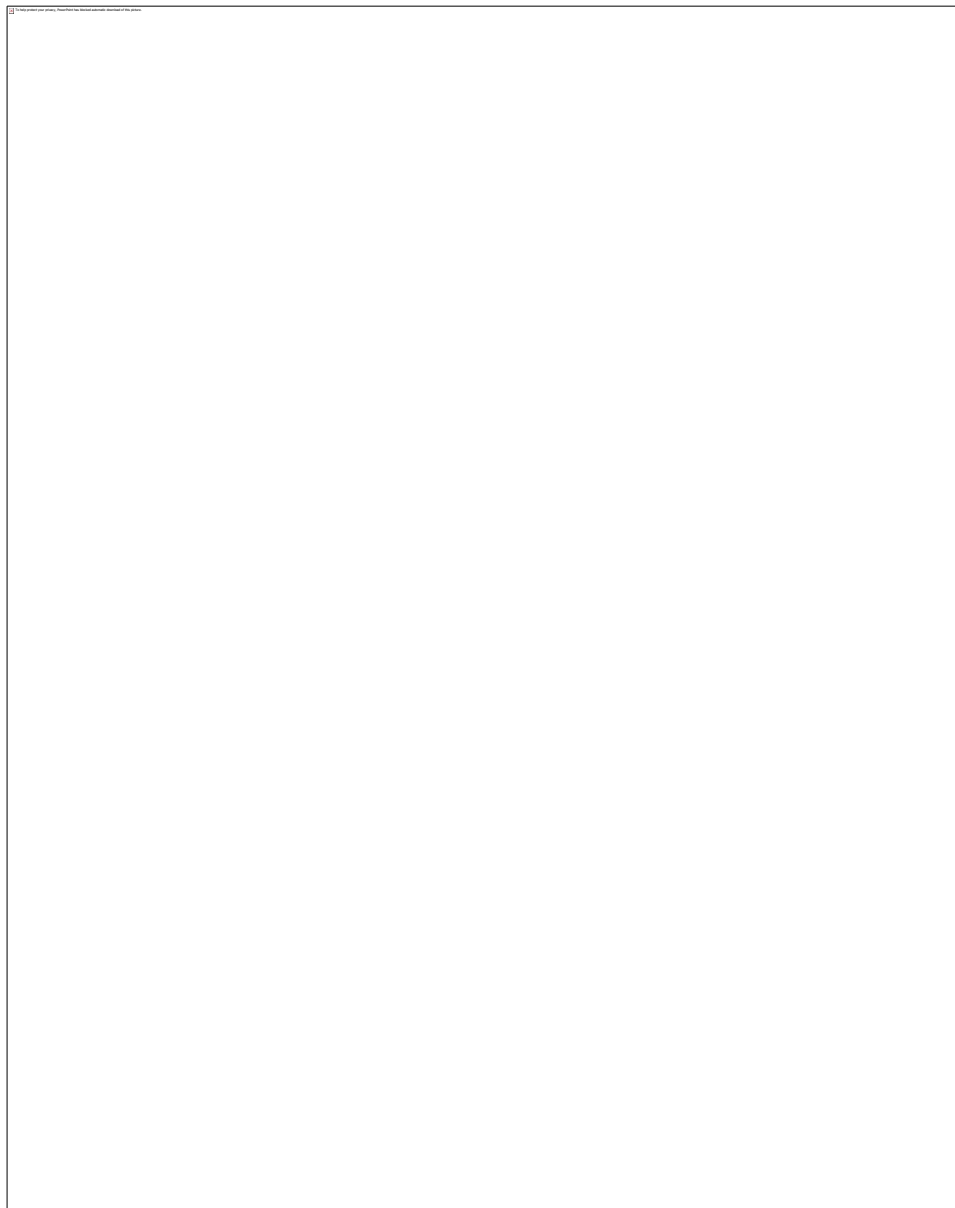
- Poor grammar and spelling;
- Blurry and pixelized logos/graphics;
- Requests that are deemed urgent, lack context and are outside of normal business operations;
- The “From” email address does not match the sender’s actual name or email address;
- Suspicious embedded URLs (hover over the link without clicking to see the actual URL address);
- Suspicious attachments with odd, unrecognizable file names.

Prevention is the Answer



7

- MFA
 - ❖ Makes it 99% less likely that you will get hacked
- Encryption
- Education
 - ❖ More than 90% of successful cyber attacks start with phishing emails
- Keep software updated
- Holidays



Headlines



9

Warren County recovering from March computer infiltration

Ransomware attack leads to shutdown of major U.S. pipeline system

Virginia Tech Says It Was Targeted in Two Recent Cyberattacks

\$600,000 payment for turf football field stolen from Spotsylvania

Smyth County Schools' computers targeted by ransomware

New Kent County Public Schools victim of ransomware attack

Fairfax County Public Schools hit by Maze ransomware

Water Plant Cyberattack Is Wake Up Call, 20 Years in the Making

10/26/2022



Why does this matter?

10

Municipalities hold significant amounts of sensitive data

- Legal
- Health
- Financial

Older, more vulnerable computer systems

Valuable data

Disruption

Virginia Public Procurement Act

Freedom of Information Act



Can you find **the**
the mistake?

<https://www.instagram.com>



Ransomware



Ransomware



13

- Ransomware is a **form of malicious software** (“**malware**”) designed to block access to a computer system or data, often by encrypting data or programs on information technology systems to extort ransom payments from victims in exchange for decrypting the information and restoring victims' access to their systems or data

Double Extortion Ransomware



14

Double extortion is a tactic wherein a crypto-malware strain steals information stored on a victim's machine before encrypting the remaining files.



The malicious actor demands payment in exchange for decryption



The malicious actor also demands payment in exchange for not publicizing the stolen data on the dark web.



Show of Hands

15

- Would your organization pay a demand?





Hypothetical Scenario

Scenario #1



17

- Ongoing construction project being done by a local construction company;
- You get an email from an “employee” of the construction company asking if the next payment could be made to an overseas account;
- What would you do?

VCU loses nearly \$500,000 in Multi-Million Dollar Cyber Fraud Scheme



18

- The real construction is company Kjellstrom and Lee;
- The scammers made their first contact with the university in September of 2018 (Rachel Moore);
- “Moore” advised the procurement department that an employee that the bank on file with the construction company was being audited and asked if the next payment could be made to an overseas account;
- After nearly three months of correspondence, the university initiated an ACH wire transfer for \$469,819.49 from their bank account on December 20, 2018, to the Bank of Hope listed in the ACH setup provided by “Moore”.

VCU loses nearly \$500,000 in Multi-Million Dollar Cyber Fraud Scheme



19

- January 2019, VCU was notified by its bank that the large wire transfer was fraudulent. The university also learned that the employee of the construction company didn't exist;
- The scammers skirted currency reporting requirements because many transfers were under \$10,000;
- See any red flags?



Hacker Changed Chemical Level in Florida City's Water System

Public wasn't in danger, Pinellas County sheriff says; investigation has been launched



Considerations



21

Sensitive, confidential or embarrassing information

Tolerance for lost data

Confidence in back-ups

Reputation

FOIA

Social Engineering



22

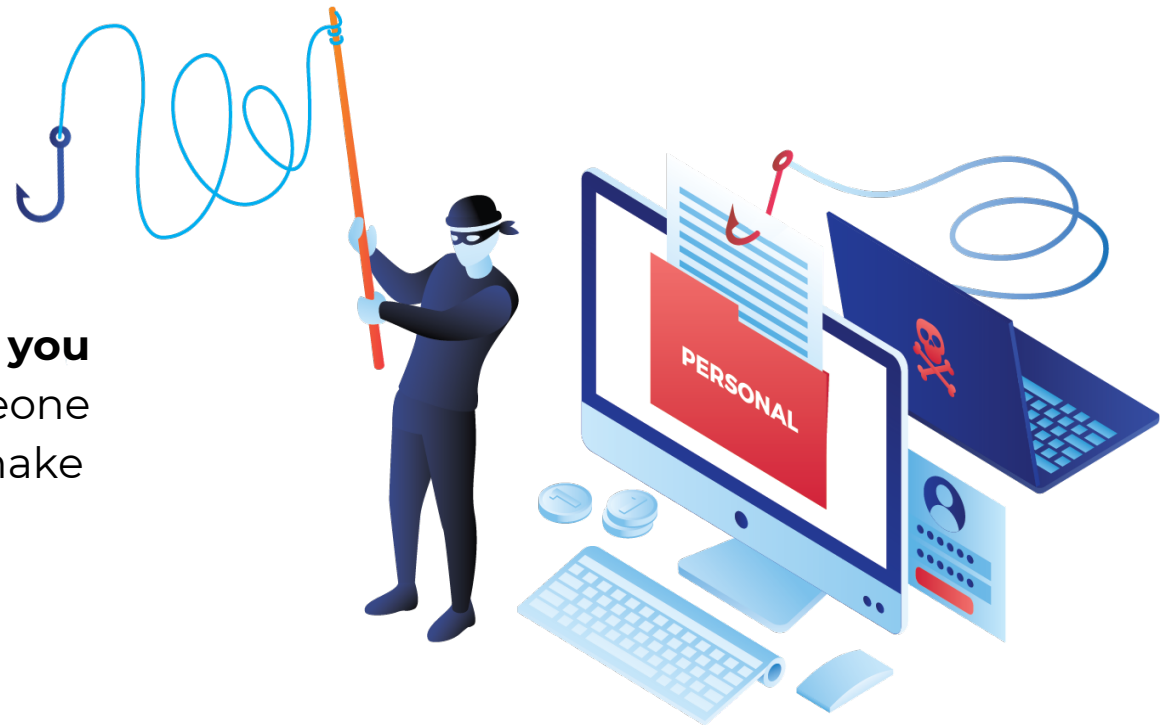
- Is about
 - Distraction and Misdirection

Phishing



23

When Scammers **fool you** to think they are someone you trust in order to make you **do something**.





7 Types of Phishing Scams

24

Email

Spear
Phishing

Smishing

Google
Search

Social
Media

QR Code

Vishing







Email Phishing Scams

25

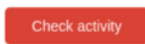
It may look like an email from your bank, Paypal, Google, Amazon, or even your CEO.

- 1 Sender Email**
Email domain is not official @google.com
- 2 Alert for immediate action**
Scams push for quick action under emotion. Instead, pause and look for red flags.
- 3 Redirect**
Hover over button reveals bit.ly link instead of official site

Subject: Critical security alert for your linked Google Account
From:  Google <google@team-support.net>



2 Sign-in attempt was blocked for your linked Google Account
 shellyteague@gmail.com

Someone just used your password to try to sign in to your account from a non-Google app. Google blocked them, but you should check what happened. Review your account activity to make sure no one else has access.

3 

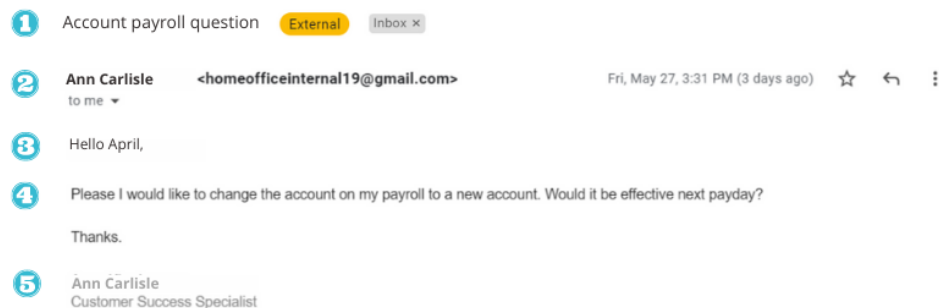
You received this email to let you know about important changes to your Google Account and services.
© 2021 Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA



Spear Phishing Scams

26

This is when they target you specifically. They have researched you, they know your family members, where you work, and who is your boss. The chances of fooling you are higher.



1 **Subject line:**
Sense of familiarity

3 **Greeting:**
Personalized

5 **Correct Job Title**
Contact name has correct job title. Spearphish attackers do their homework to look as legit as possible.

2 **Sender Name & Email:**
Sender Name is trusted name in Contacts. Email is generic Gmail instead of company email.

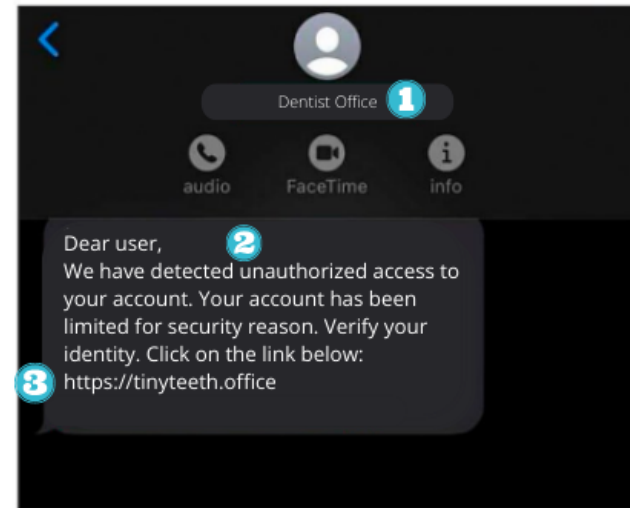
4 **Message:**
Starts a conversation to build trust before a phishing link is sent or action is requested.

Smishing Scams



27

- These are text message phishing scams. Criminals know people respond to text and instant messages faster than email.



1 Lookalike Contacts
Generic Contact Name is similar to Trusted Contact role.

2 Message
Message conveys sense of urgency and fear.

3 Lookalike URL
Scammers buy lookalike domains similar to, but different from, the real company site.

Ransomware



28

Gandcrab

(\ /) _ (\$ __ \$) _ (\ /)
●●●●●



Seller

424 posts

Joined

12/18/17 (ID: 84324)

Activity

virology

Posted 18 hours ago

Report post ↗

All the good things come to an end.

For the year of working with us, people have earned more than **\$ 2 billion**, we have become a nominal name in the field of the underground in the direction of crypto-fiber. Earnings with us per week averaged **\$ 2,500,000** .

We personally earned more than **150 million** dollars per year. We successfully cashed this money and legalized it in various spheres of white business both in real life and on the Internet.

We were glad to work with you. But, as it is written above, all good things come to an end.

We are leaving for a well-deserved retirement . We have proven that by doing evil deeds, retribution does not come. We proved that in a year you can earn money for a lifetime. We have proved that it is possible to become number one not in our own words, but in recognition of other people.

In this regard, we:

1. Stop the set of adverts;
2. We ask the adverts to suspend the flows;
3. Within 20 days from this date, we ask adverts to monetize their bots by any means;
4. Victims - if you buy, now. Then your data no one will recover. Keys will be deleted.

That's all. The topic will be deleted in a month. Thank you all for the work.

10/26/2022

Google Search Scams

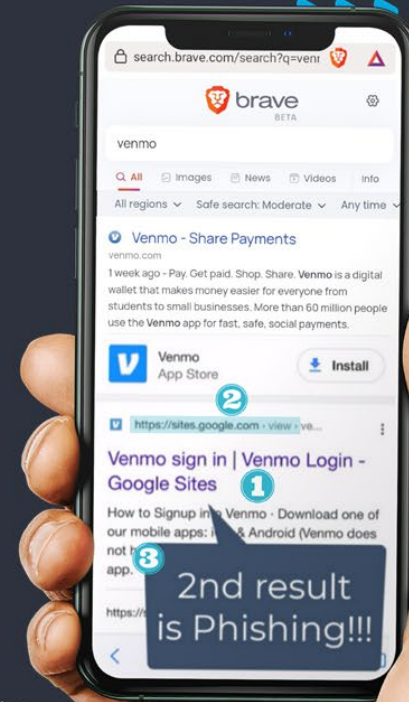


29

You may be surprised, but some of the top search results in Google are phishing links.

Scammers also invest in search engine optimization and work hard to rank their scam sites in the top search results.

- 1 Search Result Shows Brand**
Title displays correct brand name
- 2 URL Mismatch**
Title says Venmo but URL is a generic sites.google.com
- 3 2nd Result for Organic Search**
Even top search results can be manipulated for fake sites



10/26/2022



Social Media Scams

30

Social media is full of fake accounts. It could also be a fake account with the same name and photo as one of your real friends that will later try to scam you.

The screenshot displays the Instagram 'Requests' section and two message threads. In the 'Requests' section, two requests are shown: one from 'Roger H. Poast' (5 weeks ago) and one from 'Susan Beck' (7 weeks ago). Both have profile pictures and names that match real friends. The first message thread is from 'Susan Beck' (susan_beck), an Instagram account with 0 followers and 0 posts. The second message thread is from 'Roger H. Poast' (roger_h_poast), an Instagram account with 159 followers and 3 posts. Both message threads show a 'Hello' and 'How are you doing' exchange. Below the messages, there are three numbered callouts: 1. 'Known Contacts' - Friend requests from people already connected with you. 2. 'Inactive Following' - Zero or low followers is a flag especially if you know these people have been active a long time. 3. 'Odd Characters in Handle' - Both use name of the Contact with minor variation to try and avoid notice. '!' or '._'

- 1 Known Contacts**
Friend requests from people already connected with you.
- 2 Inactive Following**
Zero or low followers is a flag especially if you know these people have been active a long time.
- 3 Odd Characters in Handle**
Both use name of the Contact with minor variation to try and avoid notice '!' or '._'

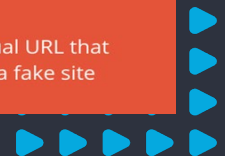
QR Code Scams



31

Who thought a QR code could be dangerous?

They are everywhere, especially in restaurants. Criminals can place their own sticker over the legitimate one. So that when you scan it, you will be redirected to a fake site.



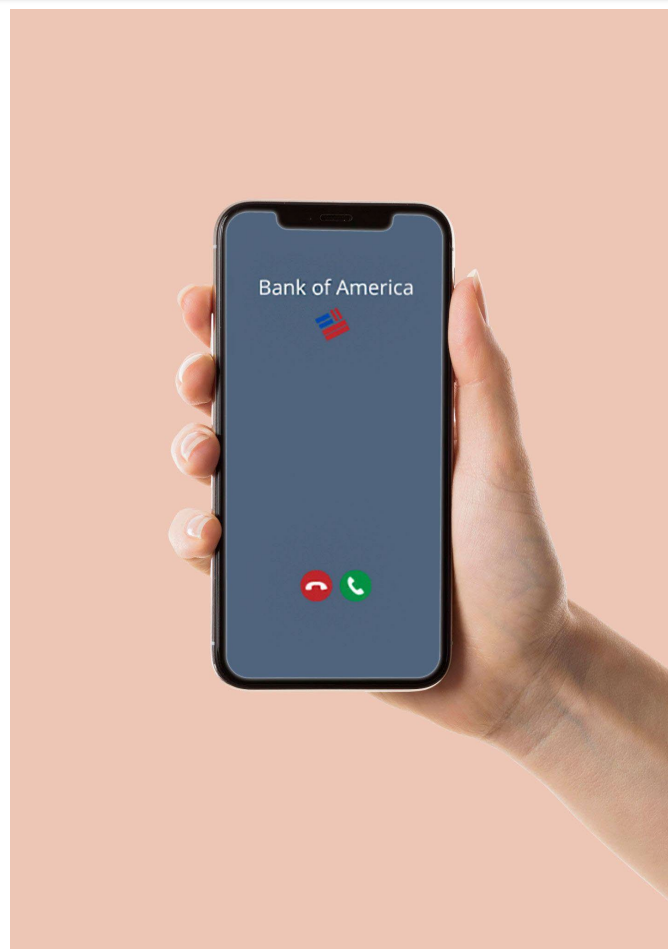


Vishing Scams

32

Vishing (voice phishing) is a type of phishing attack made over the telephone.

Scammers can spoof a phone number that looks identical to a known number, like your bank.



Social Engineering



33

OFFICE 365

Hi kinman@vmlins.org,

We detected that you have 4 delayed messages which didn't get to you. This was caused due to a system error. Rectify below:

[Release delayed messages](#)

You control the e-mail you get from Microsoft: [Unlist](#)

10/26/2022



Social Engineering

34

From: Microsoft Office [<mailto:noreply@docsecure.com>]

Sent: Wednesday, May 23, 2018 10:05 AM

To: [REDACTED] <[\[REDACTED\]@vmlins.org](mailto:[REDACTED]@vmlins.org)>

Subject: You have receive a confidential document

Importance: High

Sensitivity: Confidential



Important Document

A colleague has shared an important document with you. You may need to sign in with a Microsoft account to view the secured document.

[VIEW DOCUMENT](#)

We hope to continue serving you.

Microsoft Office

One Microsoft Way, Redmond, WA 98052

Microsoft respects your privacy. Please read our online [Privacy Statement](#).

Social Engineering



35

From: RingCentre - VMS Service <no_reply-KV38-293D0-2837DVQW@smoothstream.com.au>
Sent: Thursday, November 14, 2019 1:32 PM
To: Karen Inman <kinman@vrsa.us>
Subject: Newly arrived message_documents 6:32 PM

You have an Incoming VMS for kinman@vmlins.org,

Received- 11/14/2019, 6:32 PM

Duration- 00:35secs

PLAY

CONFIDENTIAL: The information contained in this electronic mail message is intended for the named recipients only. This message contains material that is privileged, confidential, proprietary and trade secret and otherwise protected from disclosure.

10/26/2022

Social Engineering



36

To protect your funds:

- Educate and train staff on best practices for online, e-mail, system and payments.
- Establish separation of duties requiring two or more employees to sign off on any payment.
- Validate and document any payment instructions received
- Verbally verify the request to confirm authenticity from a known number which may be different than one on the form of communication.
- Contact the entity to confirm any requests for payment method changes.
- Review all payments before they are sent and ensure all correspondence is validated and documented in a unified way.
- Slow down. Social engineering fraud often plays on inherent actions of employees.

Minimum prevention measures



37

User Education

Password
Complexity

Firewalls

Back-up key
systems and
databases

Patching



Mitigation

38

- Technical
 - ❖ Logical controls
- Physical
 - ❖ Doors
 - ❖ Servers, desktops, and laptops
- Administrative
 - ❖ Intersection of people and technology
 - ❖ Procedures
 - ❖ Training





Technical

39

From: Marcus Hensel <mhensel@vrsa.us>
Sent: Tuesday, March 30, 2021 11:09 AM
To: Jeff Thompson <jthompson@tmlirp.org>
Subject: [External]

CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

From: Virginia Risk Sharing Association [<mailto:vrsa@vrsa.us>]
Sent: Monday, March 15, 2021 2:29 PM
To: .
Subject: [EXTERNAL] VRSA Statement on COVID-19 Presumption Legislation

Caution: This email originated from a source outside of the . Do not click on links or open attachments unless you recognize the sender and you know the content is safe.

From: Lisa Schenk <lschenk@vrsa.us>
Sent: Thursday, April 15, 2021 8:56 AM
To: .
Subject: [Ext.] RE: New Marijuana Laws

CAUTION: This message has originated from an external source. Please use proper judgment and caution when opening attachments, clicking links or responding to this email.

Password Complexity



40

How long will it take to crack your password

7 characters	1 minute
8 characters	1 hour
9 characters	3-4 days
10 characters	7 months
11 characters	40 year
12 characters	2000 years

Passwords include - Lowercase, Uppercase and Numbers



A Few Last Thoughts

41

- Cybersecurity is risk management
- People, processes, technology
- If you detect an incident:
 - ❖ Immediately isolate affected system
 - ❖ Secure backups
 - ❖ Collect/review logs
 - ❖ Solicit assistance from third-party experts
- We must be perfect all the time.
- Hackers just have to be right ONCE!

CYBER RESOURCE HUB



42

- The Cybersecurity and Infrastructure Security Agency offers a range of cybersecurity assessments that evaluate operational resilience, cybersecurity practices, organizational management of external dependencies, and other key elements of a robust and resilient cyber framework. These professional, no-cost assessments are provided upon request on a voluntary basis and can help any organization with managing risk and strengthening the cybersecurity of our Nation's critical infrastructure.
- www.cisa.gov/cyber-resource-hub



43



tbullock@vrssa.us

10/26/2022