Cyber Security and Disaster Recovery

Chad Schauf

IT Director

Oakdale Electric Cooperative

MID - WEST EUUG ESRI Utility Users Group

CYBER SECURITY
WHY DO WE CARE?

Son, you're old enough now for THE TALK.
You know, about CYBER SECURITY.
Tell me what I need to know.
©MIT
PJ

This is why we care!

A November 7th 2021 Cyberattack Causes Significant Disruption at Colorado Electric Utility

The Delta-Montrose Electric Association (DMEA) CEO told local news outlets that the cyberattack led to 90% of internal controls and systems becoming corrupted, broken or disabled, and claimed that a majority of historical data dating back more than 20 years was lost.

Dec 6th New Article - Colorado cooperative Delta-Montrose Electric Association (DMEA) was hit by a "malicious" cyberattack on Nov. 7, and since then has been without payment processing, billing and other internal systems. The utility also said it suffered a significant data loss, but there was "no breach of sensitive data within our network environment" and that its distribution grid was not impacted.

July of 2021 – Rural Alabama Electric Cooperative Hit by Ransomware Attack

Wiregrass Electric Cooperative, which serves about 25,000 members, did not pay a ransom and didn't have any data compromised in the attack, chief operating officer Brad Kimbro said. Electrical service wasn't interrupted.

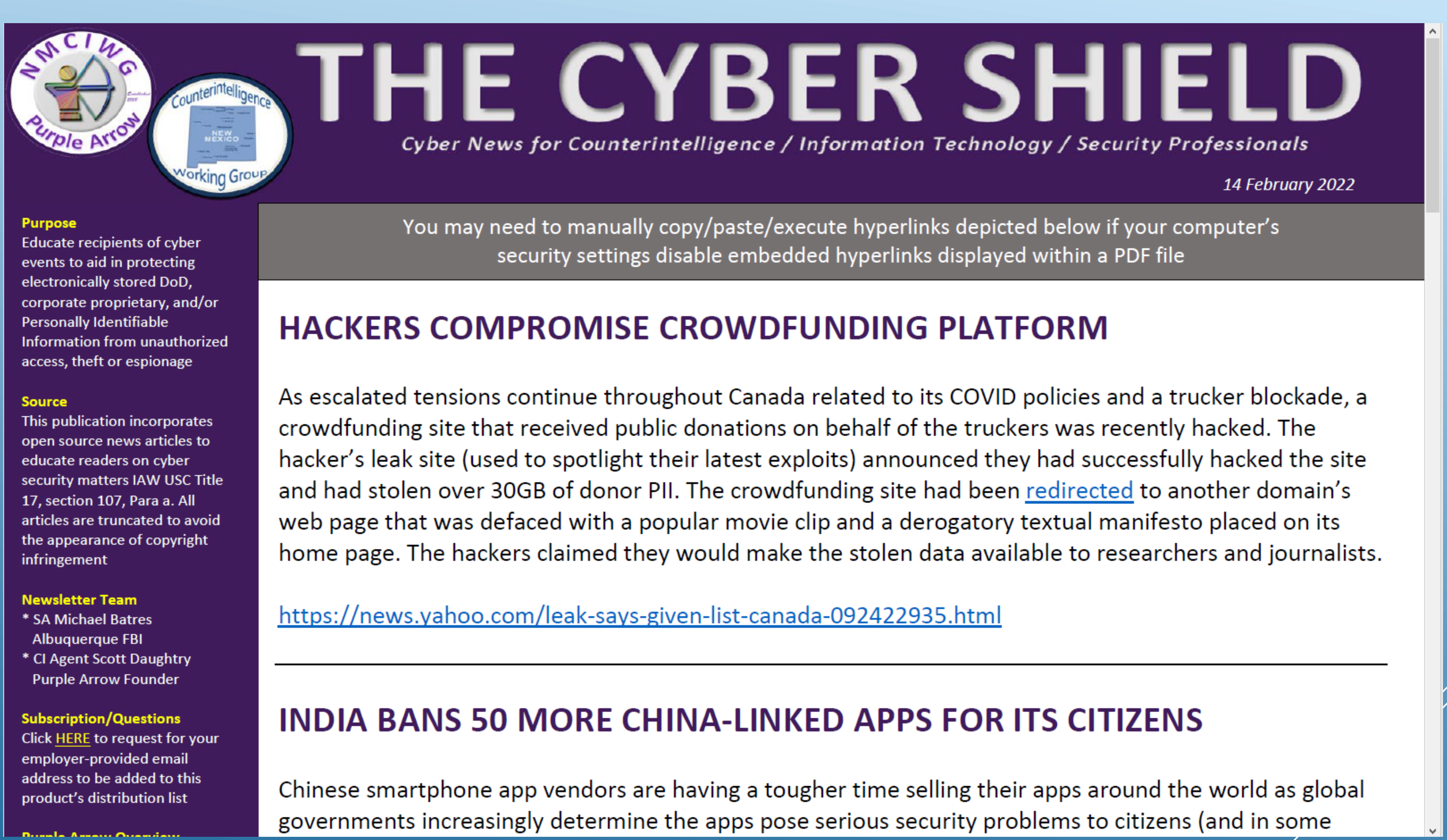
But member account information and payment systems were taken offline for maintenance and as a precaution, he said, and information technicians were starting work to reestablish customer sites.

"Our IT guys spent all weekend out of an abundance of caution looking at every server, every laptop, every computer, everything," Kimbro said.

Cyber Security Measures

- Top Tier Endpoint Protection – Zero day vulnerability protection a must!
- Multifactor Authentication
- Strong Password Policies – Minimum 15 character passwords or phrases.
- No admin rights for desktop users. Including System administrators!
- No unattended vendor access to your systems or data.
- Comprehensive backup solution, including offsite or cloud based backups
- Geo-block internet web traffic. Block the Chinese Government!
- VPN required for remote access
- Subscriptions and memberships to cyber security related organizations – E-ISAC, CISA and Infragard to name a few. The Purple Arrow is my favorite.
- Monthly Updates for all systems
- Comprehensive system documentation
- Cyber Security Incident Response Plan
- Disaster Recovery Plan
- User Training. Should include periodic phishing test campaigns.
- Periodic cyber security audits by a third party. Internal and external.
- Cyber Security Training for IT Staff

The Purple Arrow



THE CYBER SHIELD

Cyber News for Counterintelligence / Information Technology / Security Professionals

14 February 2022

Purpose
Educate recipients of cyber events to aid in protecting electronically stored DoD, corporate proprietary, and/or Personally Identifiable Information from unauthorized access, theft or espionage

Source
This publication incorporates open source news articles to educate readers on cyber security matters IAW USC Title 17, section 107, Para a. All articles are truncated to avoid the appearance of copyright infringement

Newsletter Team
* SA Michael Batres
Albuquerque FBI
* CI Agent Scott Daughtry
Purple Arrow Founder

Subscription/Questions
Click HERE to request for your employer-provided email address to be added to this product's distribution list

Purple Arrow Overview

You may need to manually copy/paste/execute hyperlinks depicted below if your computer's security settings disable embedded hyperlinks displayed within a PDF file

HACKERS COMPROMISE CROWDFUNDING PLATFORM

As escalated tensions continue throughout Canada related to its COVID policies and a trucker blockade, a crowdfunding site that received public donations on behalf of the truckers was recently hacked. The hacker's leak site (used to spotlight their latest exploits) announced they had successfully hacked the site and had stolen over 30GB of donor PII. The crowdfunding site had been redirected to another domain's web page that was defaced with a popular movie clip and a derogatory textual manifesto placed on its home page. The hackers claimed they would make the stolen data available to researchers and journalists.

https://news.yahoo.com/leak-says-given-list-canada-092422935.html

INDIA BANS 50 MORE CHINA-LINKED APPS FOR ITS CITIZENS

Chinese smartphone app vendors are having a tougher time selling their apps around the world as global governments increasingly determine the apps pose serious security problems to citizens (and in some

To Subscribe email - scott.d.daughtry.civ@mail.mil
Subject Line - SUBSCRIBE: NMCIWG Daily Cyber Newsletter

USEFUL CYBERSECURITY INFORMATION

Cybersecurity Tips

Enable installed software to perform automatic updates
Minimize the use of web browser add-ons
Research applications prior to installing them
Restrict use of Administrator-level accounts on your PC
Enable antivirus software to scan ALL files on PC
Configure antivirus software to scan attached USB devices
Scan USB thumb drives for malware prior to use
Backup important data to detachable USB drive or DVD
Ensure firmware, device drivers are updated
Enable WPA-2 encryption for your home router
-- access setting via your web browser URL ; typically via entering **192.168.0.0** or **192.168.0.1** in the address bar
Use password phrases –vs- alphanumeric passwords
Use 2-factor authentication wherever possible
Ensure family members know/use computer security

Email Phishing Indicators

Sender's email address mimics legitimate business
Generic greeting used –vs- your name
Lack of contact information within signature block
Email content misspelled your name
Email content contains poor grammar
Email content demands your urgent action
Email requests you to click an embedded hyperlink
Email requests you to read a suspicious file attachment

Your Actions:

- Confirm true destination of URL before clicking
- Manually visit the alleged sender's website
- Scan the file attachment for malware before opening
- **Notify your security/CI office of the email; they will require the original email so don't delete it**

Internet Crime Assistance

Victims of Internet Crime can request assistance from several avenues:
- The FBI's Internet Crime Complaint Center IC3
www.ic3.gov
- Their state's Attorney General office

Internet Crime involves the use of the Internet to convey false or fraudulent representation to consumers. These crimes include: willful non-delivery of goods/services, employment and/or business opportunity schemes and advance-fee schemes.

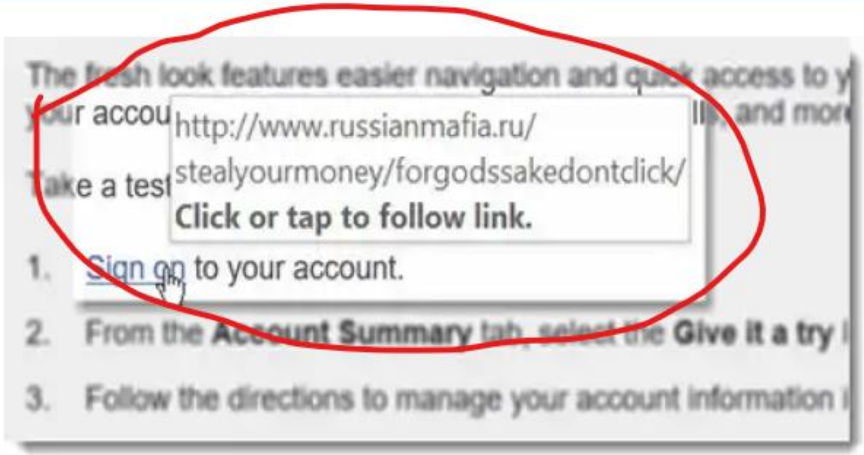
It is IMPORTANT for you to gather all relevant information related to the scheme to assist an investigation, to include receipts, original email/text messages, phone bills, etc.

Hyperlink Verification

Whenever you encounter a hyperlink embedded within a document, an email or a web page, it is CRITICAL that you verify where the hyperlink is going to send you. To do this, hover the mouse pointer over the hyperlink – the operating system should display a popup box that shows its true destination.

The example at right depicts a hyperlink associated with the text 'Sign on'; in reality, the text is linked to a web site hosted on the http://www.russianmafia.ru web site.

Also know that hackers will register domains that are similar to a known/trusted domain (for example, FBI.BIZ instead of FBI.GOV)



The fresh look features easier navigation and quick access to y
your accou ll, and more

Take a test

http://www.russianmafia.ru/stealyourmoney/forgodssakedontclick/
Click or tap to follow link.

1. Sign on to your account.
2. From the **Account Summary** tab, select the **Give it a try**
3. Follow the directions to manage your account information

That DANG Human Factor

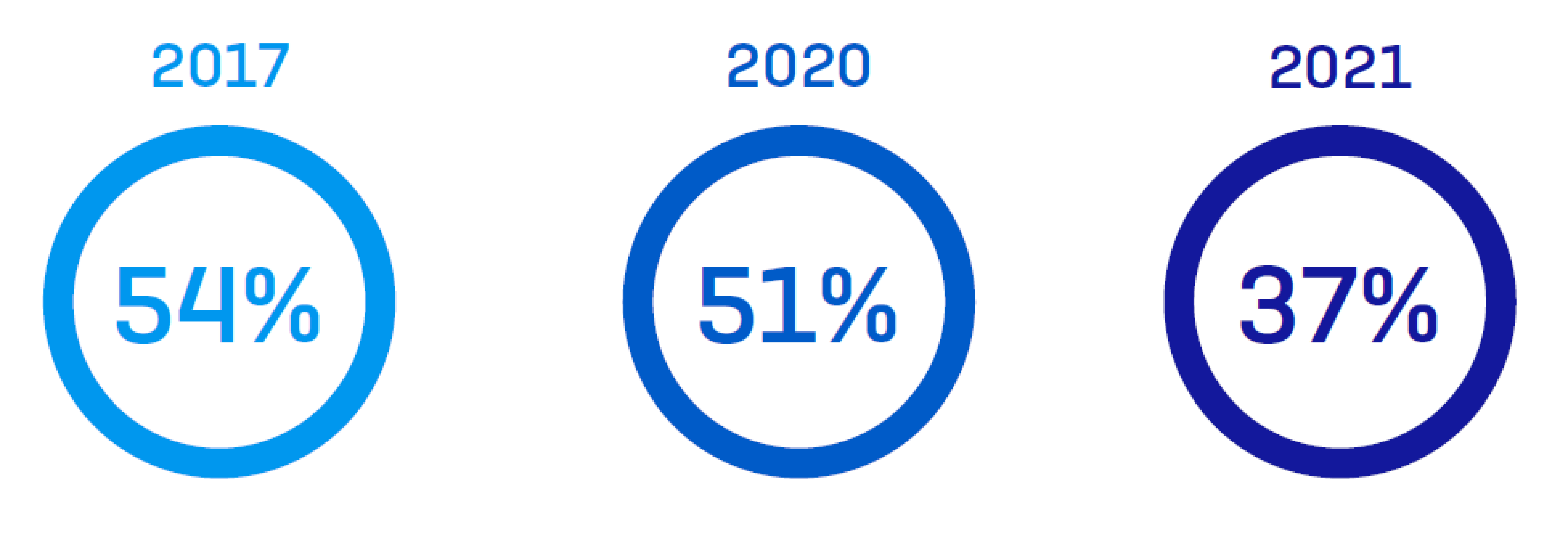
MULTI-MILLION CORPORATE CYBER SECURITY SPENDING
USER WITH LOCAL ADMIN RIGHTS OPENS EMAIL ATTACHMENT
imgflip.com

The Importance of having a Cyber Security Incident Response Plan - IRP

Sophos – The State of Ransomeware 2021

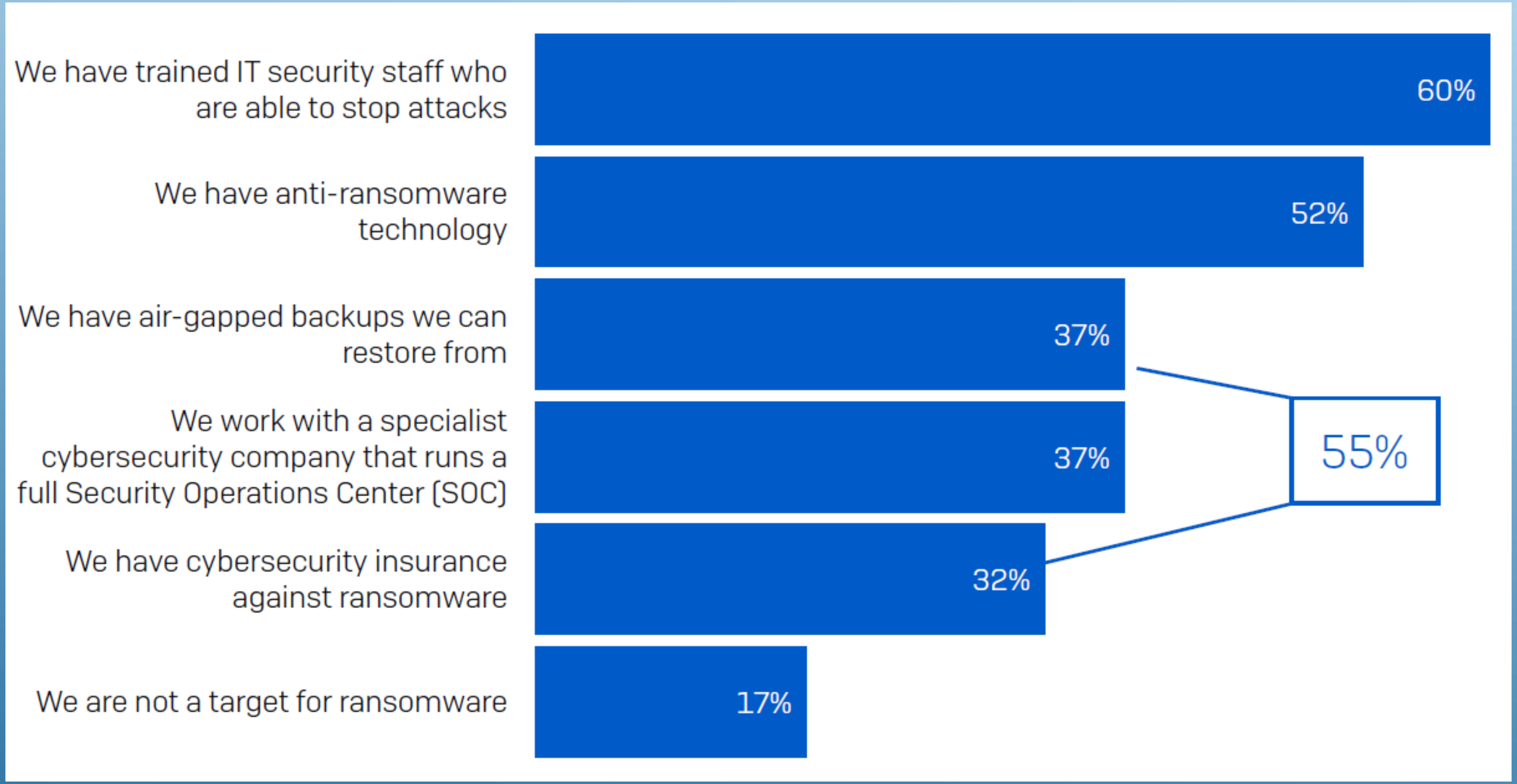
- Sophos commissioned independent research house Vanson Bourne to survey 5,400 IT decision makers across 30 countries. 197 from the Energy, oil/gas & utilities sector. The survey was conducted in January and February 2021.
- 50% of the respondents in each country came from organizations with 100 to 1,000 employees.
- 37% of respondents' organizations were hit by ransomware in the last year
- 54% that were hit by ransomware in the last year said the cybercriminals succeeded in encrypting their data in the most significant attack
- 96% of those whose data was encrypted got their data back
- The average ransom paid by mid-sized organizations was $170,404
- However, on average, only 65% of the encrypted data was restored after the ransom was paid.
- The average bill for rectifying a ransomware attack, considering downtime, people time, device cost, network cost, lost opportunity, ransom paid etc. was $1.85 million
- Extortion-style attacks where data was not encrypted but the victim was still held to ransom have more than doubled since last year, up from 3% to 7%

Ransomware remains a major threat! BUT, It’s not All Bad News……



Trained IT staff give ransomware confidence

Of those surveyed 1,166 respondents said they weren't hit by ransomware last year, and don't expect to be hit in the future. The #1 reason for this confidence in the face of ransomware is having trained IT staff who are able to stop attacks.



55% of respondents that don't expect to be hit are putting their faith in approaches that don't offer any protection from ransomware. From Sophos - Download the Full Report

Everyone Has a Plan Until They Get Punched in the Mouth – Mike Tyson Don't expect your response to go the way you think it will or should. IT WONT!

At Oakdale Electric has an IRP that has three primary documents included as a guide when responding to a basic cyber event to an all out Ransomware attack. I used example templates I got from colleagues and other cyber security resources to help me build it.

1. Cyber Incident Response Process - TOC
   - Document Purpose and Mission
   - Definitions
   - Roles and Responsibilities
   - High-level process work flow – Includes the Detection, Analysis, Containment, Eradication, Recovery phases and more. The meat of the document.
   - Appendix A – Definition of Severity
   - Appendix B – Definition of Impact

2. Ransomware Response – TOC (We felt that a document should be in place that addresses Ransomware specifically)
   - Detection and Analysis
   - Containment and Eradication
   - Recovery and Post-Incident Activity
   - Forensic Artifacts

3. Security Incident Response Form – A form fillable PDF that is available to all employees. It is to be used to report any and all cyber security events. It includes everything from the date and time, the type of incident, a description, the location and several others. It is to be used in collaboration with IT or the person responding to the event.

Download our IRP - Oakdale Electric IRP Files

I can’t compete with Todd Copeland’s dry humor but here is a shot at it! ☺

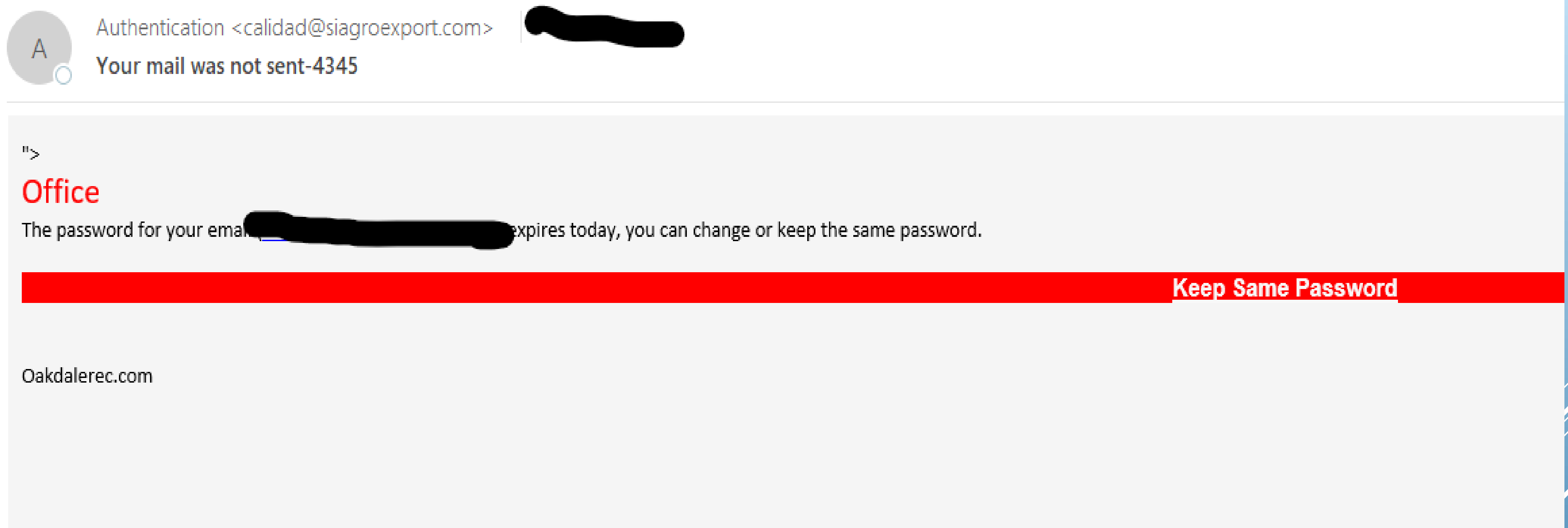
"Officer, how did the hacker escape?"

"Dunno, he just ransomware"

Tips for keeping yourself, your company and your family and friends safe!

- Don't re-use passwords
- Use complex long password phrases
- Do not open unsolicited emails. If it is at all suspicious, delete it!
- Ignore smishing text messages
- Don't click "Like" so quickly – "Like Farming" – It's a thing!
- Use as password manager – Don't save passwords in your browser. LastPass or 1Password
- Keep your devices up to date
- Backup your files
- Freeze your credit and your children's credit. "Because child identity theft schemes can go undetected for years, often until they're old enough to open up a credit card account, their data is considered especially valuable." – CNN Business
  - Security Freeze | Freeze or Unfreeze Your Credit | Equifax®
  - Credit Freeze | Freeze My Credit | TransUnion
  - Security Freeze Center at Experian

Phishing Attempt – O365 Quarantined



Authentication <calidad@siagroexport.com> [redacted]

Your mail was not sent-4345

">

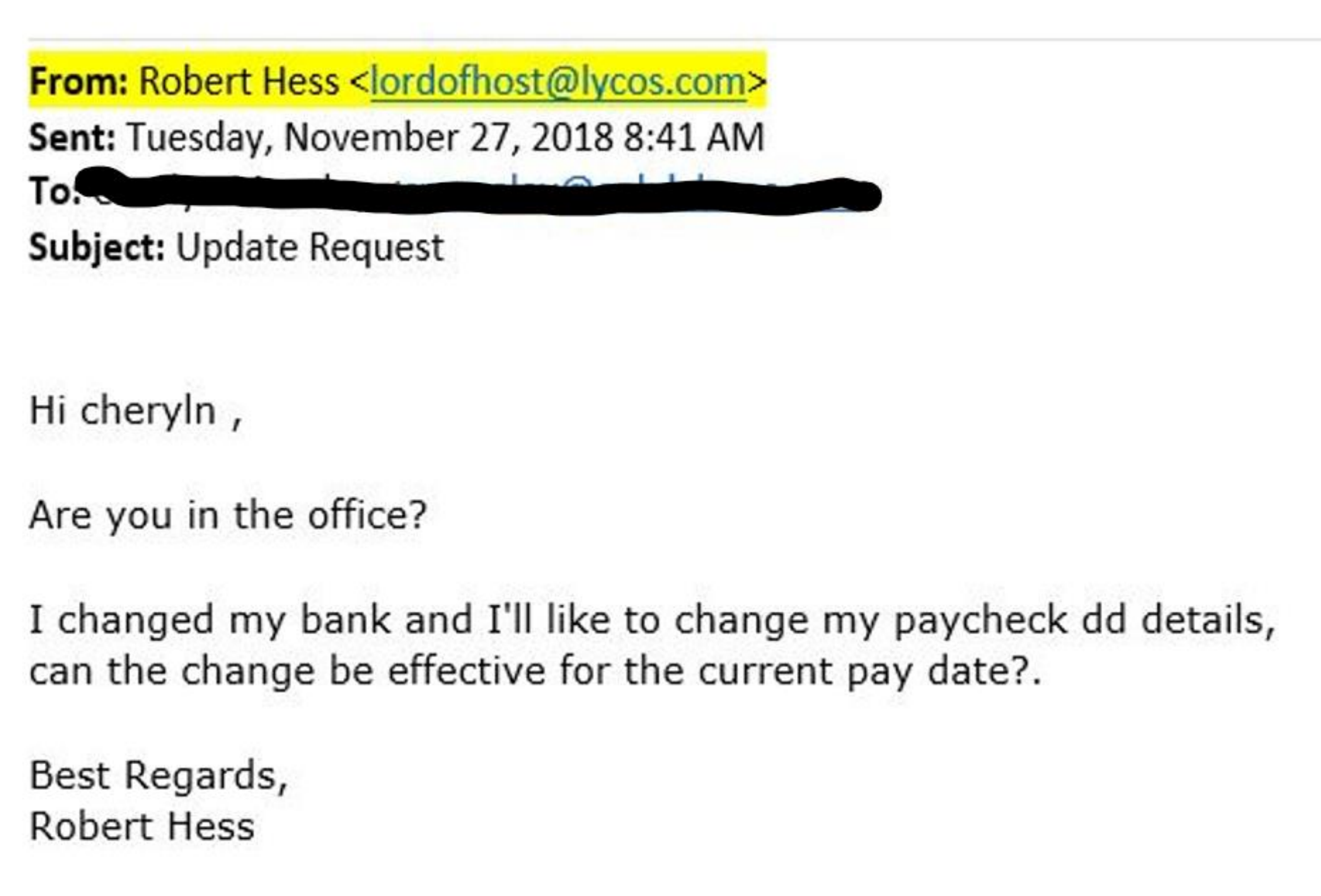
Office

The password for your emai[redacted]expires today, you can change or keep the same password.

Oakdalerec.com

According to CISCO's 2021 Cybersecurity Threat Trends report, about 90% of data breaches occur due to phishing. Spear phishing is the most common type of phishing attack, comprising 65% of all phishing attacks. The 2021 Tessian research revealed that employees receive an average of 14 malicious emails every year.

This one got through - Spearphishing



From: Robert Hess <lordofhost@lycos.com>
Sent: Tuesday, November 27, 2018 8:41 AM
To: [redacted]
Subject: Update Request

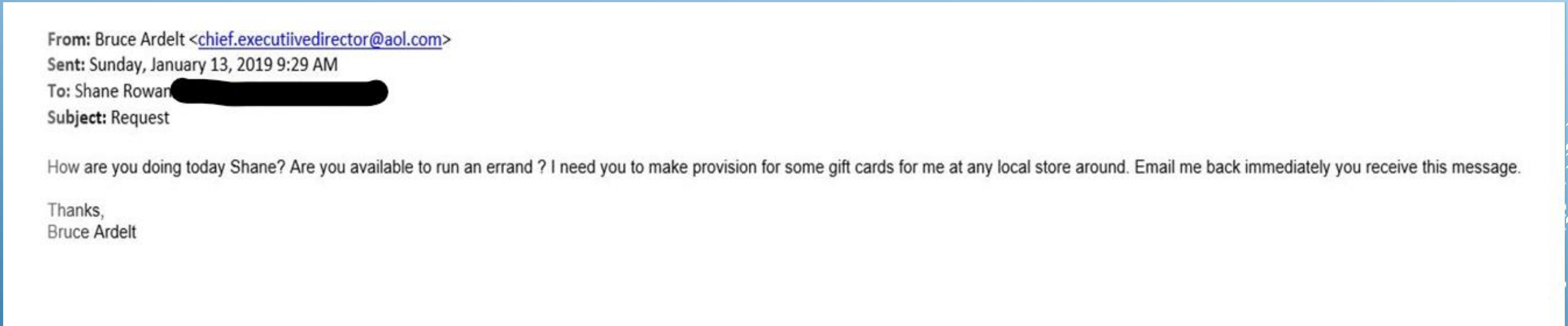
Hi cheryln ,

Are you in the office?

I changed my bank and I'll like to change my paycheck dd details, can the change be effective for the current pay date?.

Best Regards,
Robert Hess

Spearphishing

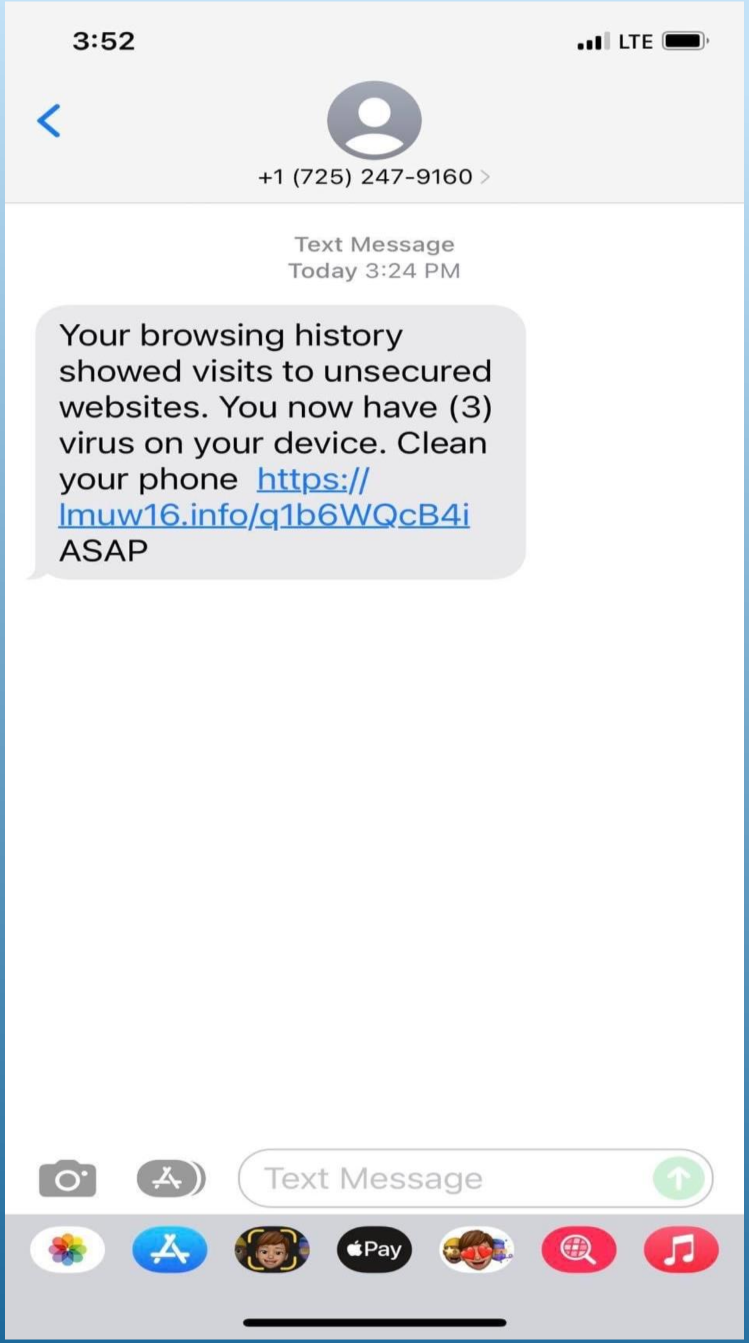


From: Bruce Ardelt <chief.executiivedirector@aol.com>
Sent: Sunday, January 13, 2019 9:29 AM
To: Shane Rowan [redacted]
Subject: Request

How are you doing today Shane? Are you available to run an errand ? I need you to make provision for some gift cards for me at any local store around. Email me back immediately you receive this message.

Thanks,
Bruce Ardelt

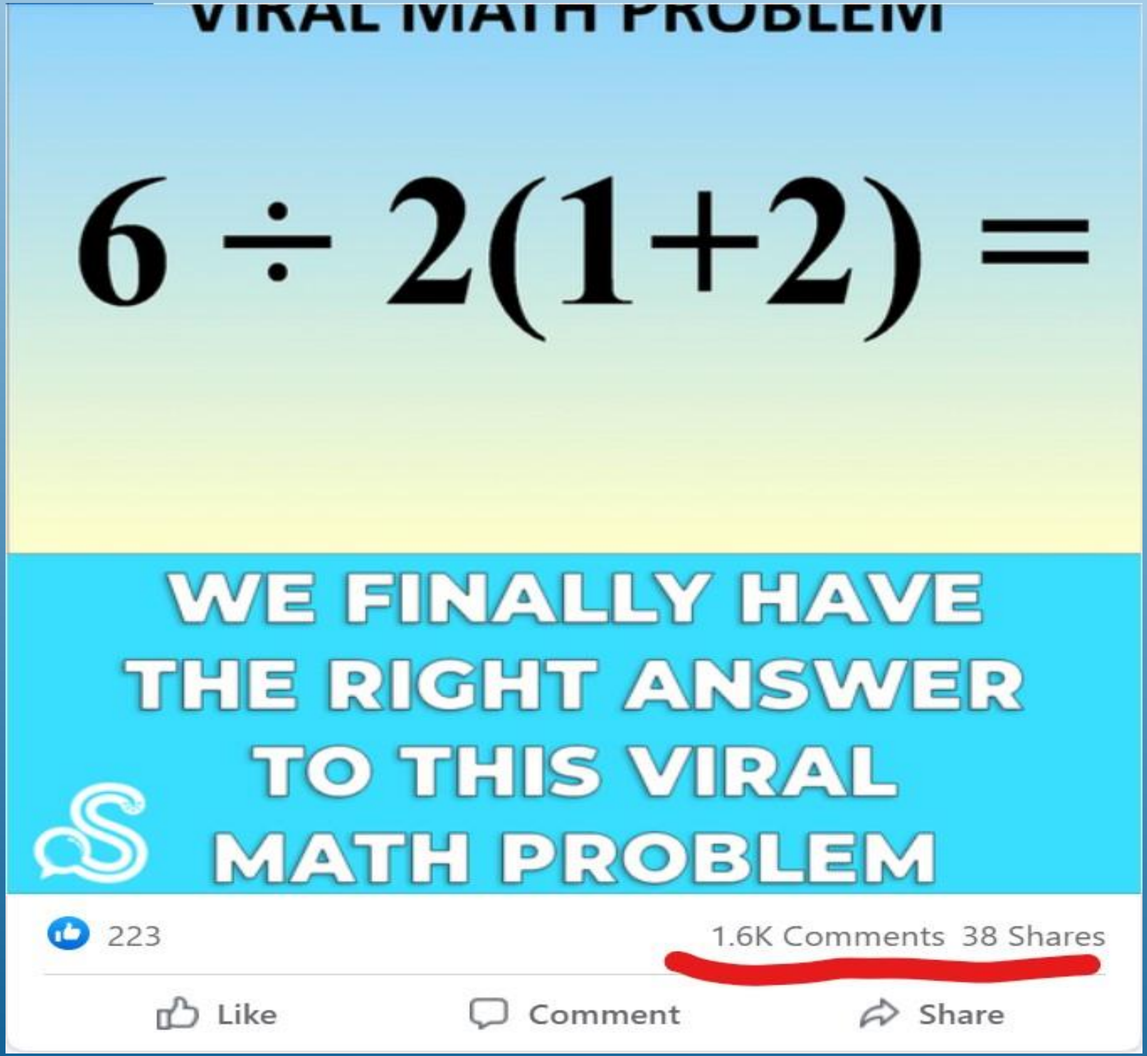
SMISHING ATTEMPT



Text Message
Today 3:24 PM

Your browsing history showed visits to unsecured websites. You now have (3) virus on your device. Clean your phone https://lmuw16.info/q1b6WQcB4i ASAP

Like Farming – Once you "like" it anyone who see's this can now see your Facebook profile! Your FB account wasn't hacked, you just liked something you shouldn't have!



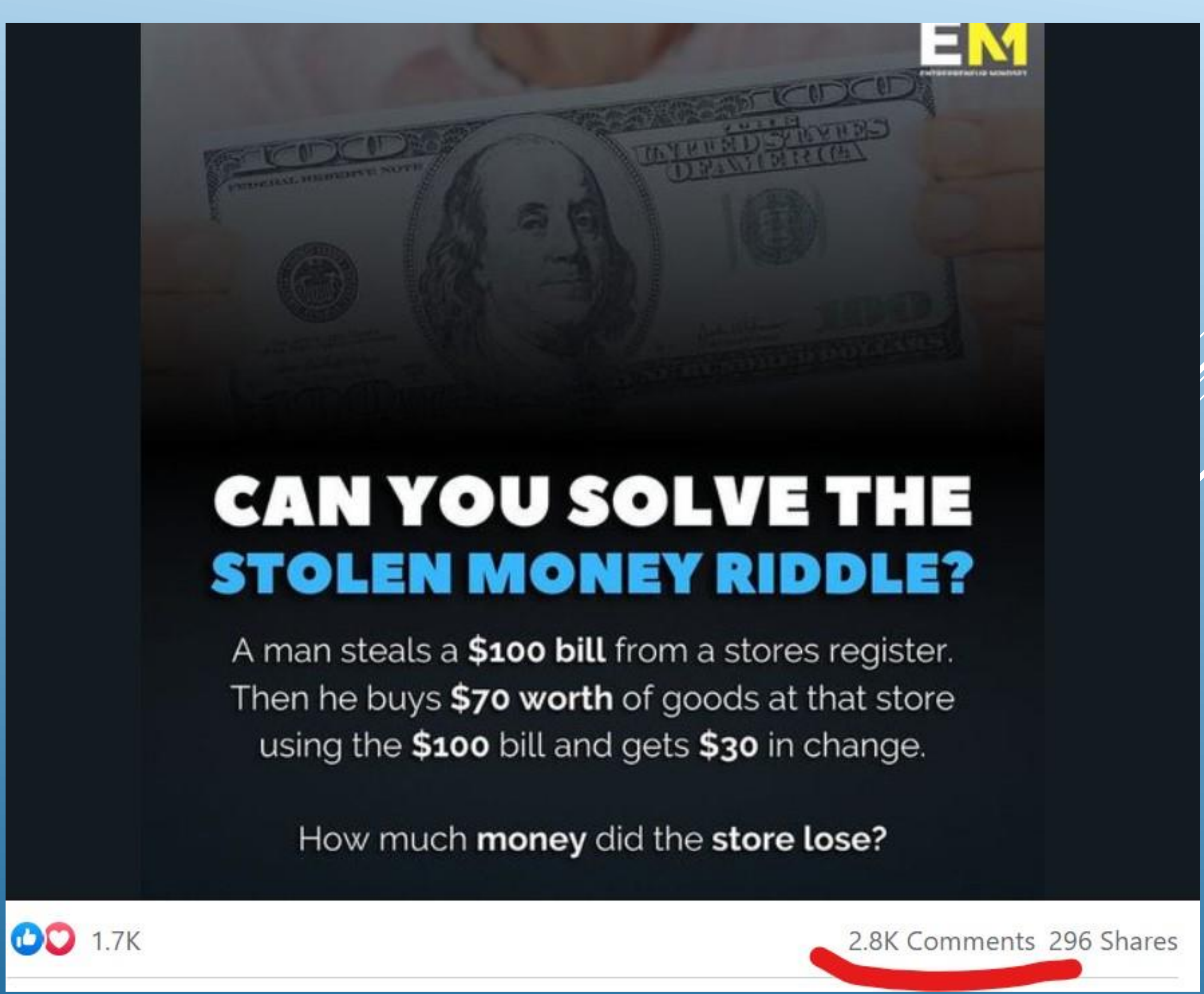
VIRAL MATH PROBLEM

$6 \div 2(1+2) =$

WE FINALLY HAVE THE RIGHT ANSWER TO THIS VIRAL MATH PROBLEM

223

1.6K Comments 38 Shares



CAN YOU SOLVE THE STOLEN MONEY RIDDLE?

A man steals a **$100 bill** from a stores register. Then he buys **$70 worth** of goods at that store using the **$100** bill and gets **$30** in change.

How much **money** did the **store lose?**

1.7K

2.8K Comments 296 Shares

Don’t Be The One!

Disaster Recovery

"TIME TO RELOCATE"
BY DIANE ALBER
I GOT THE PLUNGER!!
I KNEW PUTTING A DATACENTER NEXT TO THE BATHROOM WAS A BAD IDEA...
KIP

Disaster Recovery Defined

Wikipedia Says - Disaster recovery involves a set of policies, tools, and procedures to enable the recovery or continuation of vital technology infrastructure and systems following a natural or human-induced disaster.

Things to consider in your disaster recovery plan

- Accessible DR documentation.
- Systems Software/License information
- IT, Software and Hardware Vendor Contacts including after hours support contact numbers (Cell phones)
- Updated spare parts list
- Annual DR drill

Your plan should cover anything from Minor Data Issues to Major Data Issues

Minor data issues, such as an accidentally deleted file, are easily handled. As long as the file(s) in question has existed for at least 1 day it will be part of the nightly backups and can be found.

Major Data Issues: A major data issue constitutes a single crash, a major loss of data that spans multiple files and folders or complete loss of facilities. These are more time consuming to recover since they usually mean restoring an entire server or could also mean there are hardware replacement issues that need to be addressed.

I THINK WE MAY NEED TO UPDATE OUR DISASTER RECOVERY PLAN. THIS ONE SUGGESTS WE ALL RUN AROUND IN CIRCLES SHOUTING 'WHAT DO WE DO?!!' 'WHAT DO WE DO?!!'

DR Strategies

- Tape backups
- Backups to a disk storage device. A NAS or SAN
- Cloud backups – O365 backup strategy?
- Immutable Backups – Backup files are isolated and cannot be modified.
- USB Drives – yes a USB drive is a relatively easy way to backup your personal stuff but should never be the only strategy used.
- Server Replication – Fault Tolerance
- Alternate Backup Site Locations
- Spare hardware – Store it offsite or in a secure location outside of your server room.
- Network configuration backups – Firewall, Switches and Router configs
- Documentation
- Documentation
- Documentation
- Documentation
- Updated Documentation

Keep your plan up to date!!

Oakdale Electric is a member of an IT Shared Services group of several cooperatives geographically close to each other. Our goal is to support each other as best we can by sharing documentation, developing standards, meeting a few times a year and participating in disaster recovery drills. In 2021 we came together as a group and built a portable DR rack with spare parts. Once it was built we came up with a plan for a disaster recovery drill.

I'M NOT STUPID, OF COURSE I'VE GOT A DISASTER RECOVERY PLAN! UNFORTUNATELY IT WAS ON MY HARD DRIVE WHEN IT CRASHED.

Shared Services DR Drill

Scenario:

The test scenario for this drill involves a total failure of IT resources at the Riverland Energy's main datacenter in Arcadia, WI. This means that the local IT datacenter has been destroyed with no hardware resources available. At this point temporary IT infrastructure will be re-created from backups at one of the satellite offices. This drill is a test of that procedure to recreate the IT infrastructure and provide working systems for end users.

The Shared Services DR Rack will be utilized as a temporary network space to restore backups and get the network up and running.

Goal:

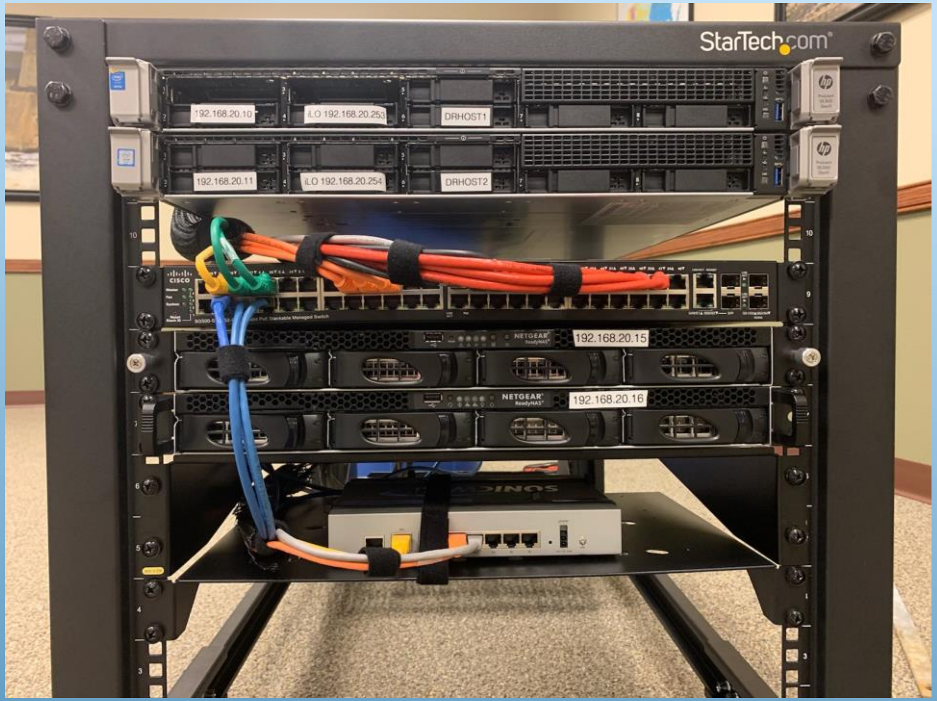
The goal of the drill was to restore and provide access to the following:

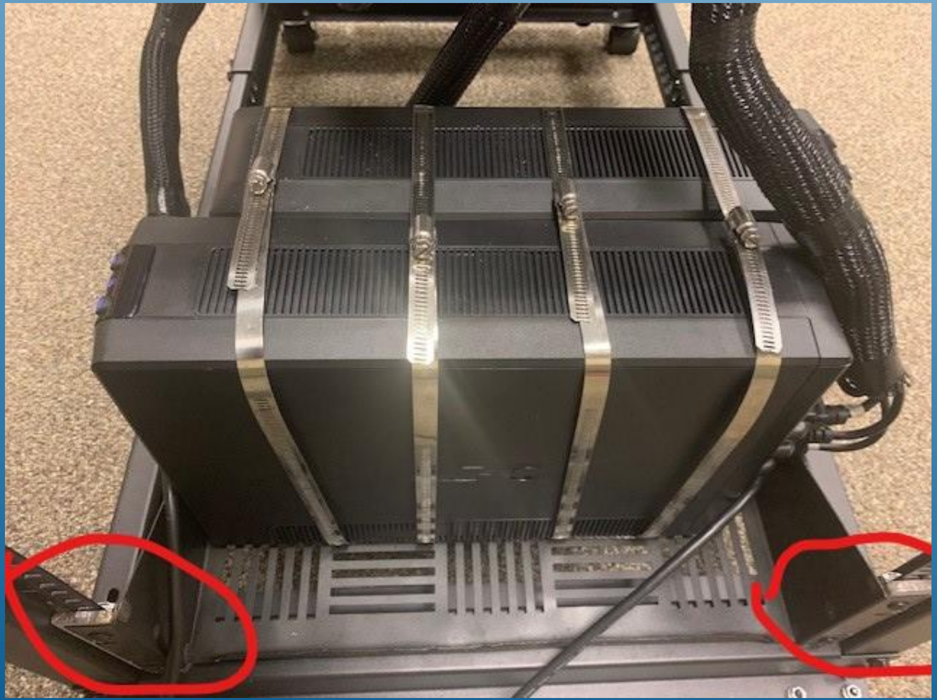
- Basic network (DNS, DHCP, Active Directory)
- iVue
- Mapping (OMS)
- Network shared drives
- At least one user PC that can access these systems

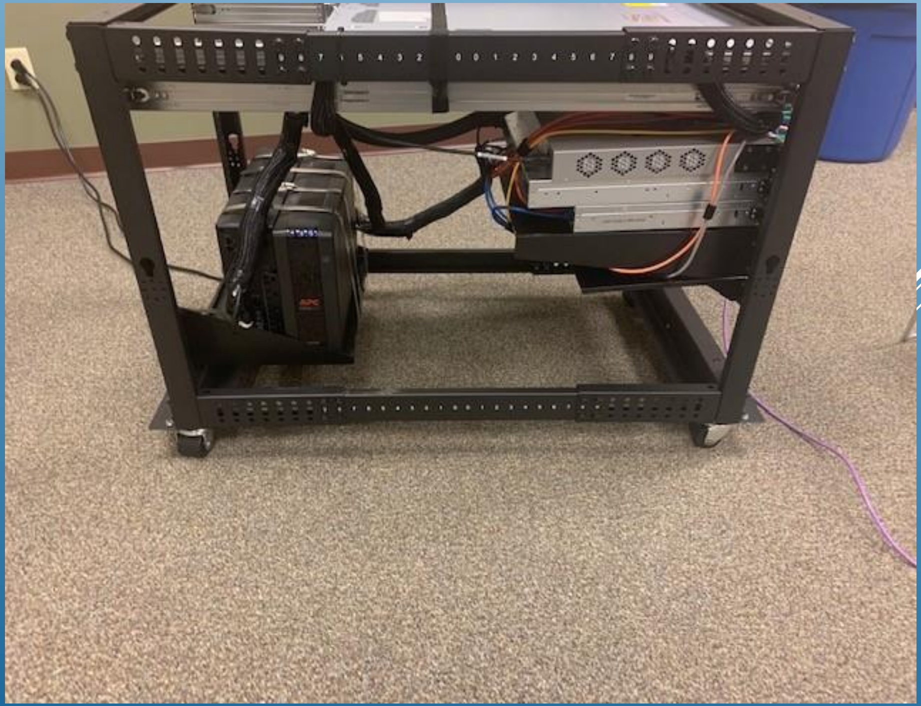
Download the entire summary - Shared Services DR Drill

The Build

Finished Product







Configuration

Questions?

Chad Schauf – cschauf@oakdalerec.com
608-372-8825

March of 2020 – The COVID Rush