If you see this screen, you are in the right place! The presentation will begin promptly at 12:00pm.

We Appreciate Your Attendance!

Hosted By:

Cliff Yount, IACCP
Vision Capital Management
Director of Compliance & Operations
November 7, 2024

# Cybersecurity

- This is an Interactive Presentation
- Hand Raise
- Chat

# As We Start, Remember These Pointers…

- BE SKEPTICAL & SUSPICIOUS OF ALL EMAILS!
- 75% of targeted cyberattacks start with an email (so we'll cover emails in-depth)!
- When in doubt, DELETE, Do Not Click or Open (go directly to the source without clicking links)!
- Be EXTRA Wary of Attachments, Links, and Hyperlinks!
- Cyber Hygiene/Clean Desk Policy (even at home)!
  - Ensure all documents with PII (Personal Identifiable Information: DOB, SSN, etc.) are cleared from areas where unauthorized individuals can gain access.

VISION CAPITAL MANAGEMENT

# What is Cybersecurity

Cyber: anything relating to the culture of computers, information technology, electronic communication networks, including virtual reality and now Artificial Intelligence (AI).

- AI is the simulation of human intelligence by software-coded evolutionary processes. AI is another tool in the cybercriminal's toolbox!
- AI can be written material or audible (impersonations)!

Cybersecurity are the actions taken to help prevent deliberate malicious attempts by other individuals or organizations (including governments) to disrupt, damage, or otherwise cause harm (often financial harm)!


VISION CAPITAL MANAGEMENT


# How do cybercriminals attack?

Social Engineering is the most common tactic…

# Social Engineering

- What is Social Engineering?
  - The use of deception to manipulate individuals into divulging confidential information to be used for fraudulent purposes.
- How does Social Engineering Happen?
  - Social Engineering is based on the human instinct of trust.
  - Cyber criminals have learned that carefully worded email, voicemail, text can convince trusting people to transfer money, provide confidential information, or download a file (malware) onto a pc or company network.
  - Cyber criminals focus on human emotions:
    - Trust, Fear, Greed, Urgency, Helpfulness, Curiosity

# Social Engineering

- Trust
- Email, Email, Email!!!
  - We are way too trusting with email!
  - We open attachments, click on hyperlinks (for efficiency to get to the proper website).
  - We respond to emails without verifying their authenticity.
  - In today's fast-paced world with the volume of emails we receive, we speed/skim read, often missing critical red flag warnings…

# Human Autocorrect

Aoccdrnig to a rscheearch at Cmabrigde Uinervtisy, it deosn't mttaer in waht oredr the ltteers in a wrod are, the olny iprmoetnt tihng is taht the frist and lsat ltteer be at the rghit pclae. The rset can be a toatl mses and you can sitll raed it wouthit porbelm. Tihs is bcuseae the huamn mnid deos not raed ervey lteter by istlef, but the wrod as a wlohe.

# Social Engineering

- Fear
- You receive a voicemail saying you're under investigation for tax fraud and must call immediately to prevent arrest and criminal investigation. This social engineering attack happens during tax season when people are already stressed about their taxes. Cyber criminals prey on the stress and anxiety of filing taxes and use these fear emotions to trick people into complying with the voicemail.

# Social Engineering

- Greed
- Imagine if you could transfer $10 to an investor and see this grow into $10,000 without any effort on your behalf. Cyber criminals use the basic human emotions of trust and greed to convince victims that they really can get something for nothing. A carefully worded baiting email tells victims to provide their bank account information, and the funds will be transferred the same day.

# Social Engineering

- Urgency
- You receive an email from customer support at an online shopping website that you frequently buy from, telling you they need to confirm your credit card information to protect your account. The email language urges you to respond quickly to ensure that criminals don't steal your credit card information. Without thinking twice, you send the information, which results in the recipient using your details to make thousands of dollars of fraudulent purchases.

# Social Engineering

- Helpfulness
- It's human nature to want to trust and help one another. After researching a company, cyber criminals target two or three employees with an email that looks like it comes from the targeted individuals' manager. The email asks them to send the manager the password for the accounting database – stressing that the manager needs it to ensure everyone gets paid on time. The email tone is urgent, tricking the victims into believing they are helping their manager by acting quickly.

# Social Engineering

- Curiosity
- Cyber criminals pay attention to events capturing a lot of news coverage and then take advantage of human curiosity to trick victims into acting.
- For example, after the second Boeing MAX8 plane crash, cyber criminals sent emails with attachments that claimed to include leaked data about the crash. The attachment installed a version of the Hworm RAT on the victim's computer.

# Common Cyber Attacks: Phishing (not fishing)

# Common Cyber Attacks - Phishing

- Phishing is the practice of sending fraudulent email that appear to come from a reputable source. The goal is to steal sensitive data (PII, credit card numbers, login information) or to install malware on the victim's machine. Phishing attempts can often come in a spoofed email.
- What is spoofing/spoofed email?
  - A technique used in phishing attacks to trick users into thinking the message is from a person or entity they know or trust.
  - The sender forges email headers, specifically the email address.

# Common Cyber Attacks - Phishing

- You receive an email from a seemingly familiar enterprise that you deem legitimate, such as your bank, university or a retailer you frequent. The message directs you to a site—usually to verify personal information such as email addresses and passwords—that then steals your information and exposes your computer to attack by scammers.
- Phishing scams are some of the most common attacks on consumers. According to the FBI, more than 114,700 people fell victim to phishing scams in 2019. Collectively, they lost $57.8 million, or about $500 each.

# Common Cyber Attacks - Phishing

- Phishing emails and text messages (smishing) frequently tell stories to trick people into clicking on a link or opening an attachment. For example, phishing attempts may:
  - Say they've noticed suspicious activity or log-in attempts on your account
  - Claim there's a problem with your account or payment information
  - Say you need to confirm or update personal information
  - Include a fake invoice
  - Ask you to click on a link to make a payment
  - Claim you're eligible to sign up for a government refund
  - Offer a coupon for free goods or services

# Common Cyber Attacks - Phishing

- You should never click the links provided in emails you can't independently confirm. Doing so will make your computer and personal information vulnerable to viruses and malware. Again, though the sender may seem legitimate—which is exactly what the scammer wants you to believe—no reputable institution will ask for your password or other key personal information online. Phishing emails will often contain typos or grammatical errors, and the sender's email address often looks suspicious.
- Phishing emails are often rife with typos and grammatical errors. This is an intentional strategy scammers use to "weed out" people who would be unlikely to fall for the scam.

# Common Cyber Attacks – Quid Pro Quo

- A back and forth, exchange of information where the cyber criminal will provide information or a service in return for your information.
- Typically, Quid Pro Quo criminals don't perform any advanced targeted research of their victims and offer to provide a service or assistance, assuming identities like tech support professionals.

# Common Cyber Attacks - Malware

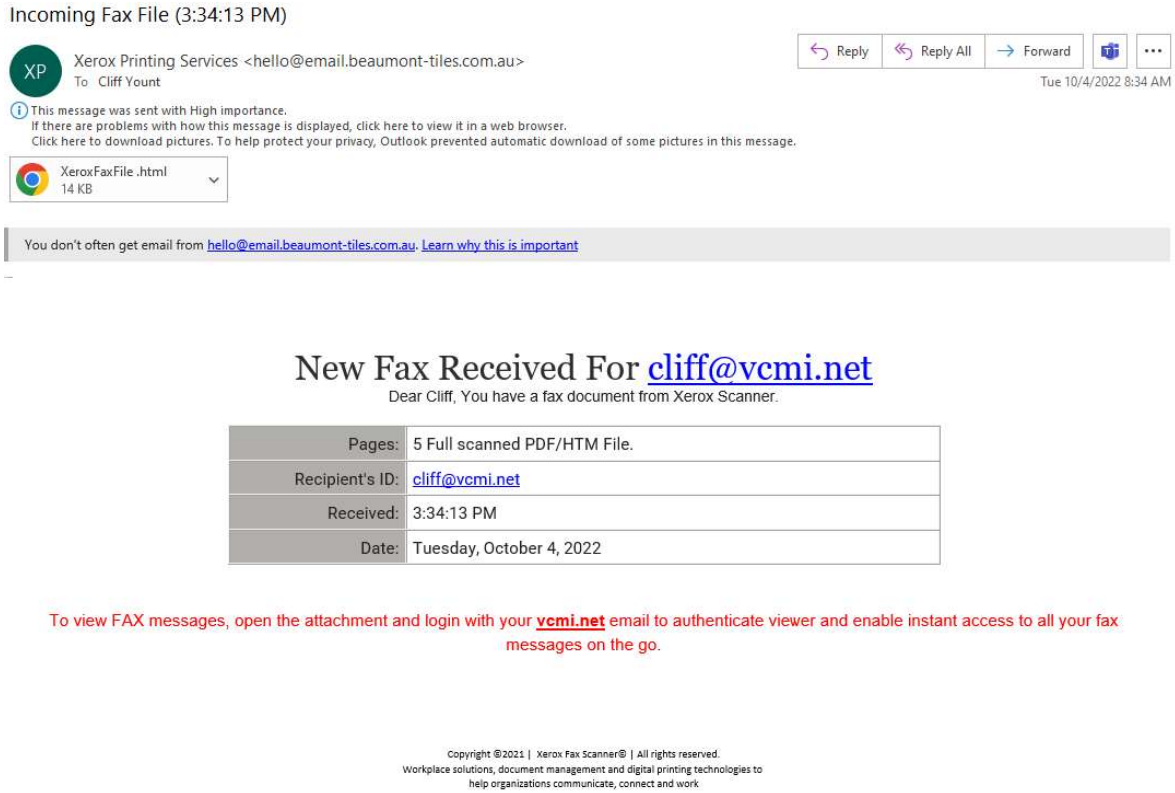
- Malware is malicious software, including spyware, ransomware, viruses, and worms. Malware breaches a network through a vulnerability, typically when a user clicks a dangerous link or email attachment that then installs risky software. Once inside the system, malware can do the following:
  - Blocks access to key components of the network (ransomware)
  - Installs malware or additional harmful software
  - Covertly obtains information by transmitting data from the hard drive (spyware)
  - Disrupts certain components and renders the system inoperable

# Common Cyber Attacks - Malware

- Victims are sent an urgently worded message and tricked into installing malicious software "malware" on their device.
- Popular tactic is telling the victim that malware has already been installed on their computer and the sender will remove the malware if they pay a fee.
- Dormant Malware - Hybernates

# Phishing/Spoofing Examples…

# Spoofing/Phishing



Incoming Fax File (3:34:13 PM)

XP

Xerox Printing Services <hello@email.beaumont-tiles.com.au>
To Cliff Yount

Reply | Reply All | Forward

Tue 10/4/2022 8:34 AM

This message was sent with High importance.
If there are problems with how this message is displayed, click here to view it in a web browser.
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

XeroxFaxFile .html
14 KB

You don't often get email from hello@email.beaumont-tiles.com.au. Learn why this is important

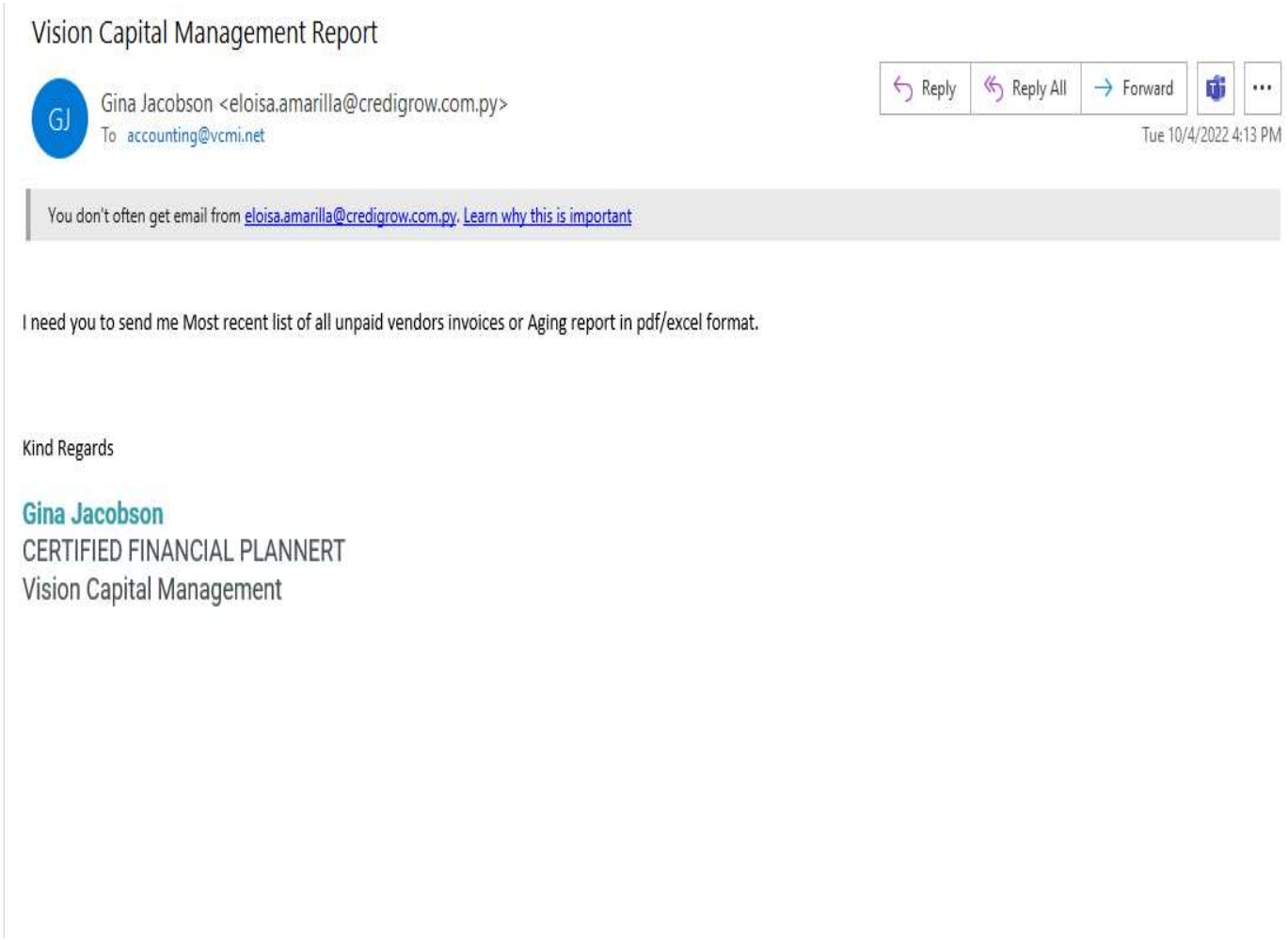
New Fax Received For cliff@vcmi.net

Dear Cliff, You have a fax document from Xerox Scanner.

| | |
|---|---|
| Pages: | 5 Full scanned PDF/HTM File. |
| Recipient's ID: | cliff@vcmi.net |
| Received: | 3:34:13 PM |
| Date: | Tuesday, October 4, 2022 |

To view FAX messages, open the attachment and login with your **vcmi.net** email to authenticate viewer and enable instant access to all your fax messages on the go.

# Spoofing/Phishing



Vision Capital Management Report

GJ

Gina Jacobson <eloisa.amarilla@credigrow.com.py>

To accounting@vcmi.net

Reply | Reply All | Forward | ...

Tue 10/4/2022 4:13 PM

You don't often get email from eloisa.amarilla@credigrow.com.py. Learn why this is important

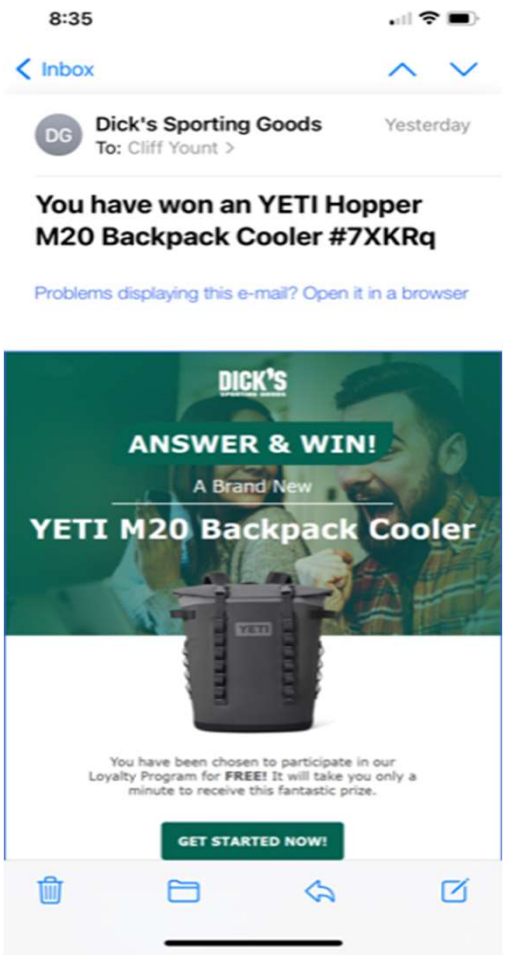
I need you to send me Most recent list of all unpaid vendors invoices or Aging report in pdf/excel format.

Kind Regards

Gina Jacobson
CERTIFIED FINANCIAL PLANNERT
Vision Capital Management

# Spoofing/Phishing

- Fake shopping websites and formjacking.
- Email on Your Phone: Can you tell if it's Legit or Fake?

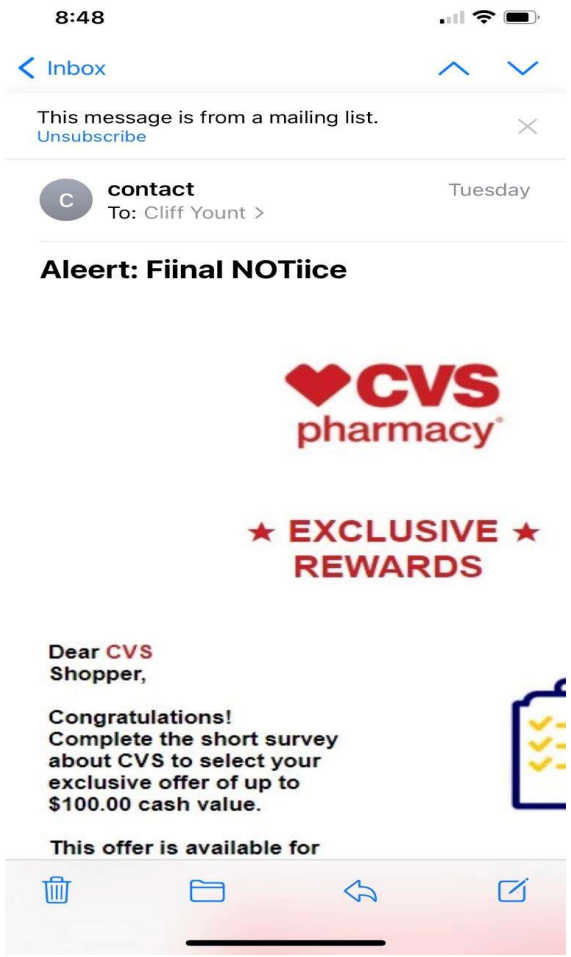


# Fake Shopping Websites and “Formjacking”

- Thousands of fake websites offer "great deals" on well-known brands. These websites typically have URLs similar to the brands they try to mimic, such as "Amazon.net." If you buy something from one of these websites, chances are you'll receive a counterfeit item in the mail—or nothing at all.
- Formjacking is another retail scam that happens when a legitimate retail website is hacked, and shoppers get redirected to a fraudulent payment page, where the scammer steals your personal and credit card information.
- To avoid this scam, double-check that the URL on the payment page is the same as the website where you were shopping. Cybercriminals may change the URL very slightly—maybe by adding or omitting a single letter. Be sure to take a close look at the URL before you enter your payment details.

# Formjacking Examples…

- Fake shopping websites and formjacking.
- Email on Your Phone: Can you tell if it's Legit or Fake?



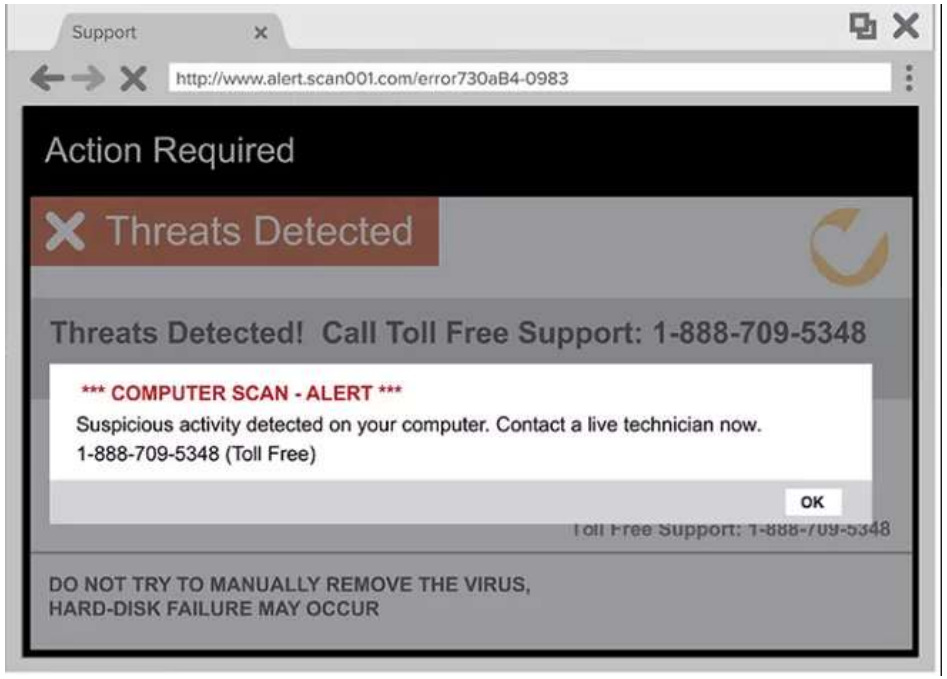
# Other Fraudulent Scams…

# Scareware

- Fake Antivirus Software (aka 'Scareware')
- Fake antivirus software ads and pop-ups try to make you believe your computer is infected with a virus (or dozens of them)—and that you can fix the problem by downloading their software. These scammers get you two ways:
  - They gain access to your credit card information.
  - They gain access to your computer. When you click the download link, you get a virus, malware, or ransomware instead of antivirus software.
- Always be wary of ads and pop-ups that prompt you to take immediate action, or ones that are hard to close.
- Be sure to install, update, and use real antivirus software to reduce the risk of scareware.

# Scareware - Tech Support Scams

- With this scam, you receive a phone call, email, or pop-up warning indicating your computer is infected (ask yourself: How would they know?). The scammer then:
  - Prompts you to download an application that allows them to control your computer remotely;
  - Downloads an actual virus or otherwise makes you believe that something is wrong; and
  - Tells you they can fix the problem for a fee.
  - Often, these scammers ask you to pay using a bank wire, gift card, or money transfer.



# Grandparent Scams

- A fraudster poses as a panicked grandchild who needs cash right away for some emergency—to get out of jail, to leave a foreign country, or to pay a hospital bill.
- Grandparent scams are on the rise, with losses in the millions annually.
- Resist the urge to act immediately. Scammers pull at your heartstrings and rely on you to respond quickly—before you've had a chance to think things through.
- Verify the caller's identity. Ask questions that a stranger wouldn't be able to answer.
- Confirm the story with other family members or friends, even if (or especially if) the caller says to keep it a secret.
- Never send cash, gift cards, or money transfers.
- Using AI (60 Minutes)

VISION CAPITAL MANAGEMENT

# Other Financial Scams

- **Bogus government sources.** These scammers claim to issue updates and payments on behalf of the Internal Revenue Service (IRS) or local tax authority.
- **Fraudulent financial offers.** Scammers may pose as banks, debt collectors, or investors, designed to steal financial information.
- **Fake nonprofit donation requests.** Many people like to donate to charitable causes to help with disaster relief. This provides an excellent opportunity for scammers to set up fake organizations to collect funds. Donate directly through a reputable nonprofit's website instead of clicking on a link you receive by email or text.
- **Fake Amazon Employees –** 1/3 of business-impostor fraud complaints involve scammers claiming they're from Amazon.
- **P2P (Peer to Peer) Payment Requests –** Scammers are increasingly demanding payment via money transfer like Venmo, Zelle, etc. It's so convenient — you pay in seconds from your phone or computer. But these payments usually can't be canceled.
- **Tax Impostors -** Scammers are impersonating the IRS as well as state, county and municipal law enforcement and tax collection agencies to get you to share sensitive personal information or send money to settle your tax debt. They may call, email, or mail letters threatening to revoke your driver's license or passport. Some pretend to offer state tax relief.
- **Disaster Relief Scams; Pre-Approved Notices; Debt Relief/Credit Repair Scams**

VISION CAPITAL MANAGEMENT

# What to do if Victimized?

- If a virus or malware is suspected, DO NOT turn off your device. Do not attempt any further keystrokes and enlist the help of an expert.
- Change all of your passwords immediately (ideally from another machine). This should be a routine practice (& do not use the same password for different sites).
- Set up account alerts. Monitor your financial accounts by setting up alerts to warn you when any important changes are applied to your account.
- Exercise vigilance with your online presence. Limit what you share on social media and set privacy and security settings on websites and applications to safeguard your information.
- Monitor account activity regularly. Make a habit of reviewing your financial account statements and online activity. Confirm that you recognize all the transactions listed—and report any that you don't.

# What to do if Victimized?

- Depending on severity of the hack, you may want to freeze your credit and call your credit card company, if necessary.
- If warranted, contact your local law enforcement authorities to report the scam and get help with the next steps.
- You can also report the scam to the FBI, the Federal Trade Commission, the U.S. Postal Inspection Service, and your state attorney general's office.

# CyberTips

- BE SUSPICIOUS OF EVERYTHING!
- When in doubt, DELETE!
- Clean Desk Policy – at home and work!
- If you connect it, protect it – Phones, laptops, tablets, etc., make sure they are up to date with all patches and add anti-virus software.
- Use a password keeper and don't use the same password across sites.
- Update passwords regularly.
- Don't click on links you're not expecting.
- Unsubscribe from email distributions making your inboxes easier to navigate. Make sure the UNSUBSCRIBE link is legit.
- Contact the "author" by calling the person or business directly if an email or voicemail seems suspicious.

# Cybersecurity Tips

- Stay current on the latest scams. Educate family and friends on scams you are aware of. Especially kids/young adults who utilize their phones for EVERYTHING! The more we all know, the better off we'll all be!
- The weakest points of any cybersecurity are us humans. Educating those you work and socialize with may save you from receiving spam/phishing down the road.
- Don't provide any PII…DOB, SSN, Bank Account Info, address over the phone, email or internet unless you know it's a legitimate request.
- It's safe to assume that if anyone is asking for your bank or personal information, you're being scammed. You should never give out personal information to anyone on the internet who contacts you directly. If you have to make a financial transaction online, make sure you're doing so on a secure server and through a reputable site.

# As We Finish, Remember These Pointers…

- ALWAYS BE SUSPICIOUS & Continue to be Educated!
- Don't Be Alarmed (or overwhelmed by all of these examples)! Rather, simply be SKEPTICAL & SUSPICIOUS OF EVERYTHING ONLINE!!!
- When in doubt, DELETE, Do Not Click or Open!
- Be EXTRA wary of Links & Hyperlinks!

# Questions…

- If someone is calling from a bank or another place I conduct business, asking to verify PII, how do I confirm the request is legitimate?
  - Request their contact information, hang up, return call to a number YOU know.
- Antivirus/malware software brand recommendations?
  - Reputable brands only: Norton, Malwarebytes, Bitdefender, TotalAV, Webroot.
  - MAKE SURE to keep up with the software security updates.
- Firewall Recommendations
  - Reputable brands only: Barracuda, Ubiquiti, Cisco, Sonic Wall, Netgate, Fortigate.
  - MAKE SURE to keep up with the security updates (software & firmware).
- Password protectors, third party apps (Block Party)?
  - Research, research, research!

# Further Questions?

- CLIFF YOUNT
- CLIFF@VCMI.NET
- 503-731-7309
- Contact me anytime!