



DEFEND AGAINST CLEVER CYBER SCAM ATTACKS

5/31/2022

TODAY'S AGENDA

Moderator



Ron Samson
Demand Generation Manager

Webinar Speaker



Dave Jooste
Owner

1. About NIP Group
2. What is a Cyber Scam
3. Complexity and Identification
4. Scam Response
5. Follow-up Mitigation
6. Q&A





CYBER TECH CONNECTION

ADVANCED TECH SUPPORT & CYBERSECURITY

WWW.CYBERTECHCONNECTION.COM

CYBER SCAM ATTACKS

- 
- INTRODUCTION
 - What is Cyber Scam Attack?
 - COMPLEXITY AND IDENTIFICATION
 - Vulnerabilities enabling scam delivery
 - Common route of delivery
 - SCAM RESPONSE
 - Type of response
 - Technical knowledge
 - FOLLOW-UP MITIGATION
 - System defense
 - Monitoring

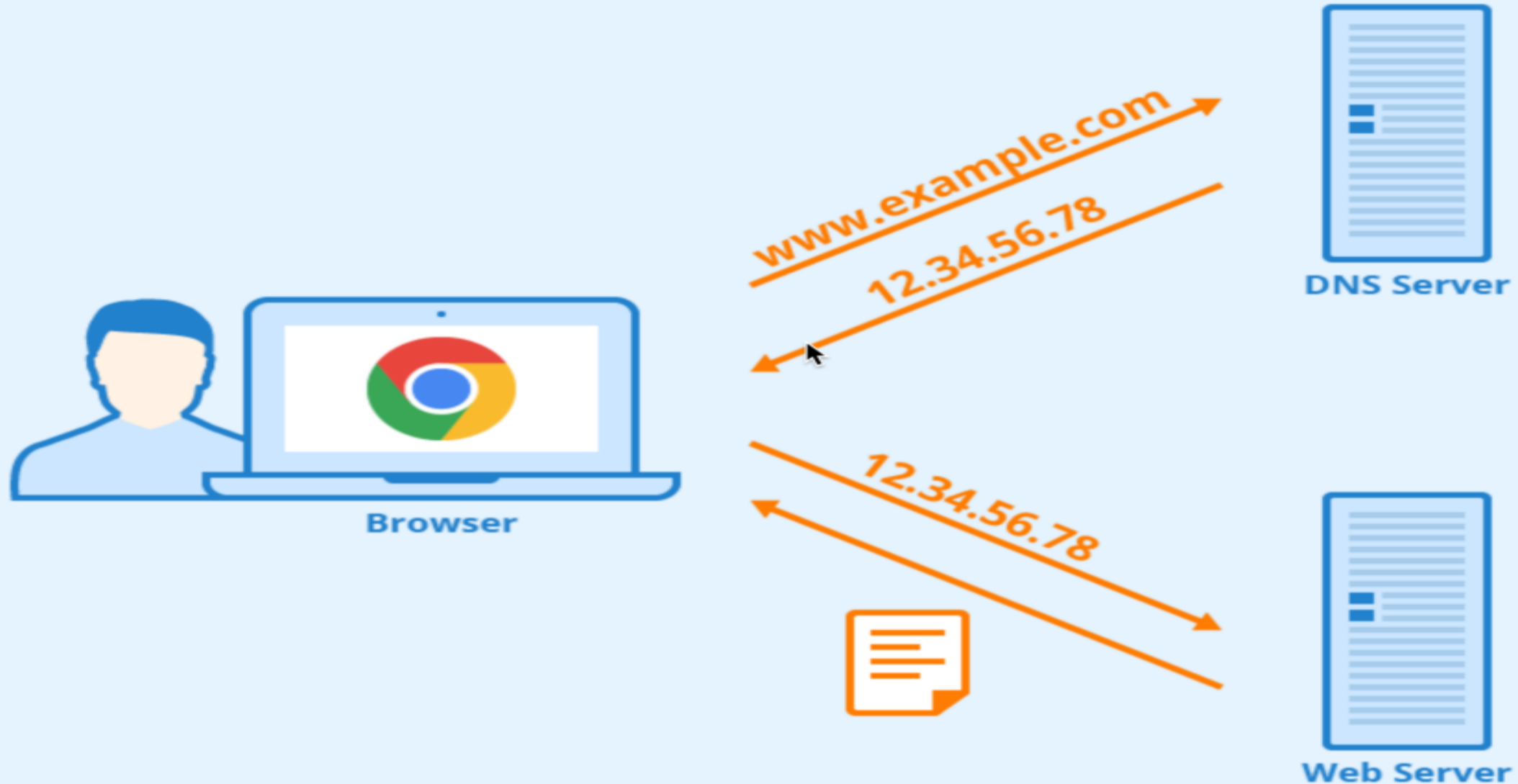
WHAT IS A CYBER SCAM?

Cyber security is broad in its applications and defenses, however cyber scams are also broad. We will cover the most common cyber scams.

- Types of clever cyber scams
 - Mobile Scams
 - Social Media & Engineering Scams
 - Fake Anti-Virus Scams
 - Phishing Scams

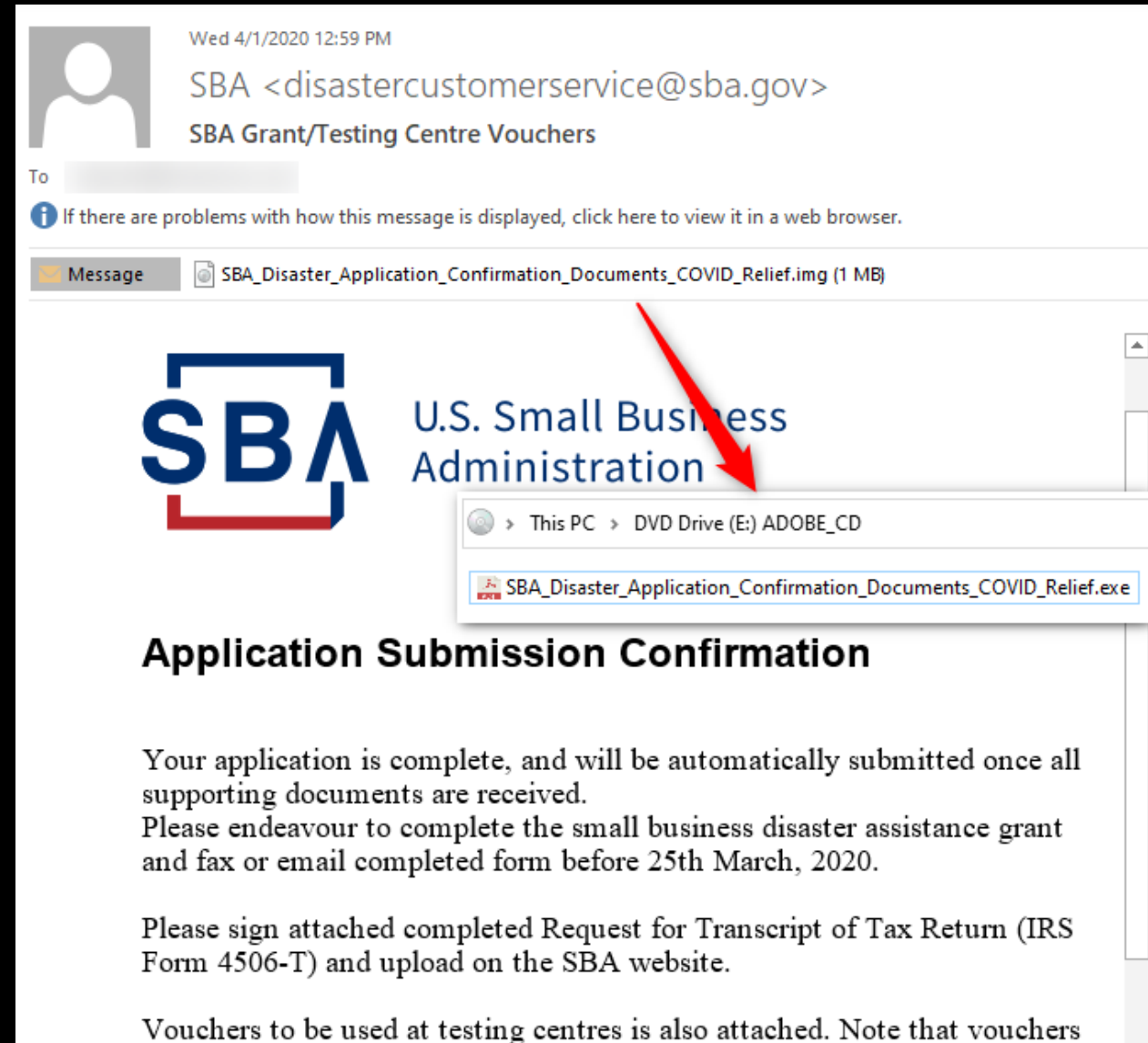


COMPLEXITY & IDENTIFICATION



VULNERABILITY & SCAM ENABLING

- I DID NOT KNOW MY DNS COULD BE EXPOSED!
- **DNS SPOOFING:** The coronavirus period has made life tough on businesses.
 - The phishing emails impersonate the US Small Business Administration (SBA), and are aimed at delivering malware, stealing user credentials or committing financial fraud.
- **I DID NOT KNOW!**
 - Sometimes tech experts forget simple measures.
 - DNS fixes can take as little as 15 minutes to correct.



COMMON ROUTE OF DELIVERY

WITH MOST SCAM ATTACKS THERE IS ALMOST ALWAYS A COMMON ACTIVATOR

MOBILE SCAM: “click here to claim your prize”

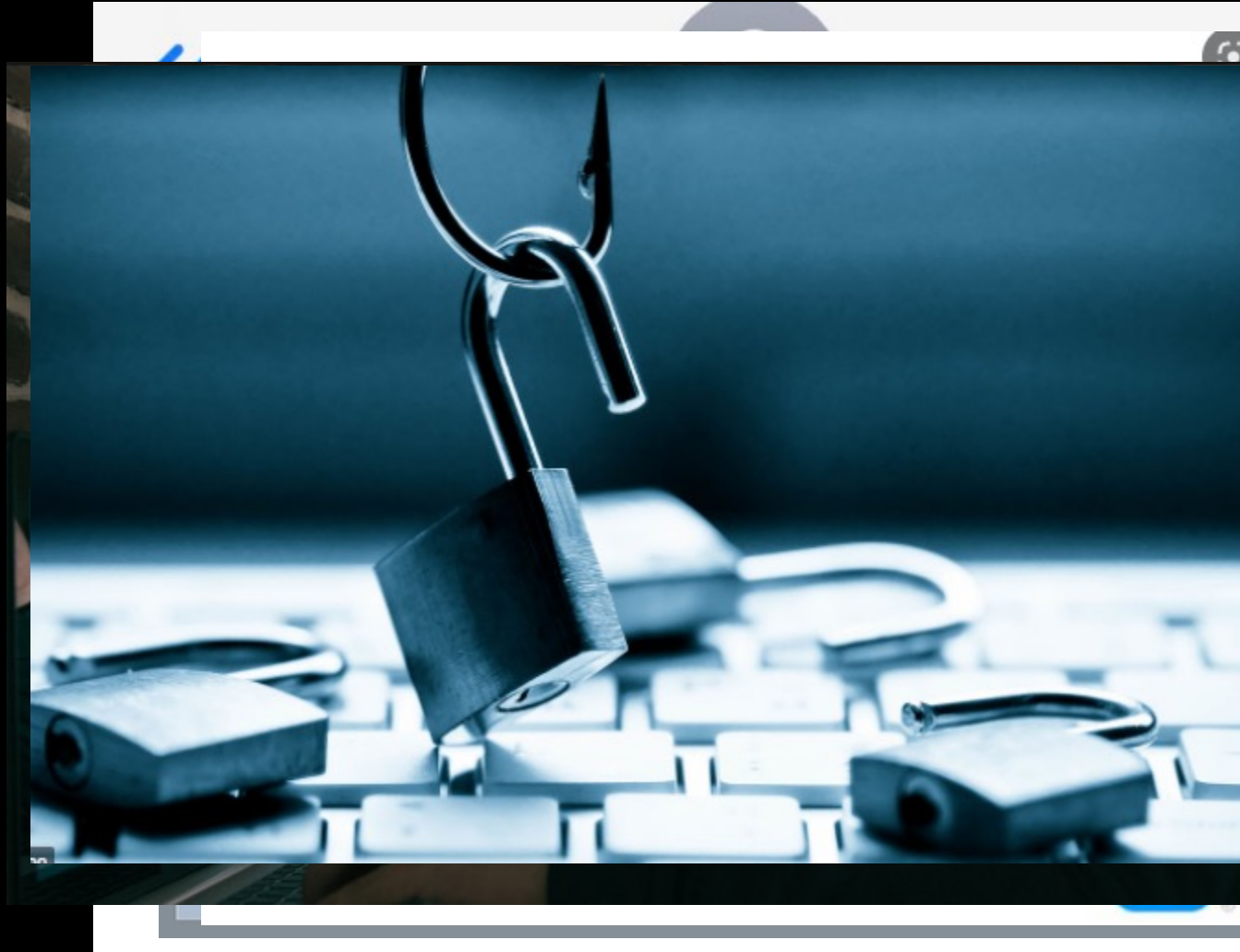
FAKE ANTIVIRUS: “activate your copy here”

SOCIAL MEDIA: “accept this offer or click here to view who viewed your profile”

SOCIAL ENGINEERING: Includes phone calls to and from fake numbers provided by hackers.

PHISHING: “secure your account here”

At least 90% of CLEVER scams involve the end-user clicking a URL link



SCAM RESPONSE & TECHNICAL KNOWLEDGE

If you suspect you are a victim of a scam, you have a **very small window to act**.

MOBILE SCAM: Delete the text and block the sender. Change the password for the affected account.

FAKE ANTIVIRUS: Turn off your P.C location services. Install a real anti-virus program.

SOCIAL MEDIA: Reset your social account passwords and enable MFA

SOCIAL ENGINEERING: Question who the caller is and **TRUST** your instincts. Don't be bullied by the speaker.

PHISHING: Act quickly and reset passwords. Enable MFA and conditional access policies. Check DNS settings.



ALWAYS RESET PASSWORDS FOR ANY SUSPECTED COMPROMISED ACCOUNT

BUSINESS ACCOUNTS SHOULD PURCHASE CYBER INSURANCE

FOLLOW-UP MITIGATION

SYSTEM DEFENSES:

Vulnerability testing: Have your IT vendor run system scans or 3rd party vulnerability assessments

Secure Antivirus: Tough question – no anti-virus is 100% secure, however many are above standard.

Account Controls: Account controls usually require some sort of approval or authentication before changes are made.

MFA: A must for all online accounts, especially email, domain, and social media accounts.

MONITORING:

Technical Control: There are many. A deeper understanding of your IT network is required for this

Alerts: If you are action-orientated, then this is for you. These assist in staying ahead of breaches.

Cyber Breach Action Plan: What do to in a breach or scam. Many insurance companies now require this.

3rd Party Monitoring: Most small businesses don't have the resources to handle all things IT, so many outsource and often reduce their overhead.

CALL SOMEONE FOR HELP IF YOU NEED TO!

Q & A

Moderator



Ron Samson
Demand Generation Manager

Webinar Speaker



Dave Jooste
Owner

Thank you for attending our Defend
Against Clever Cyber Scam Attacks webinar.

