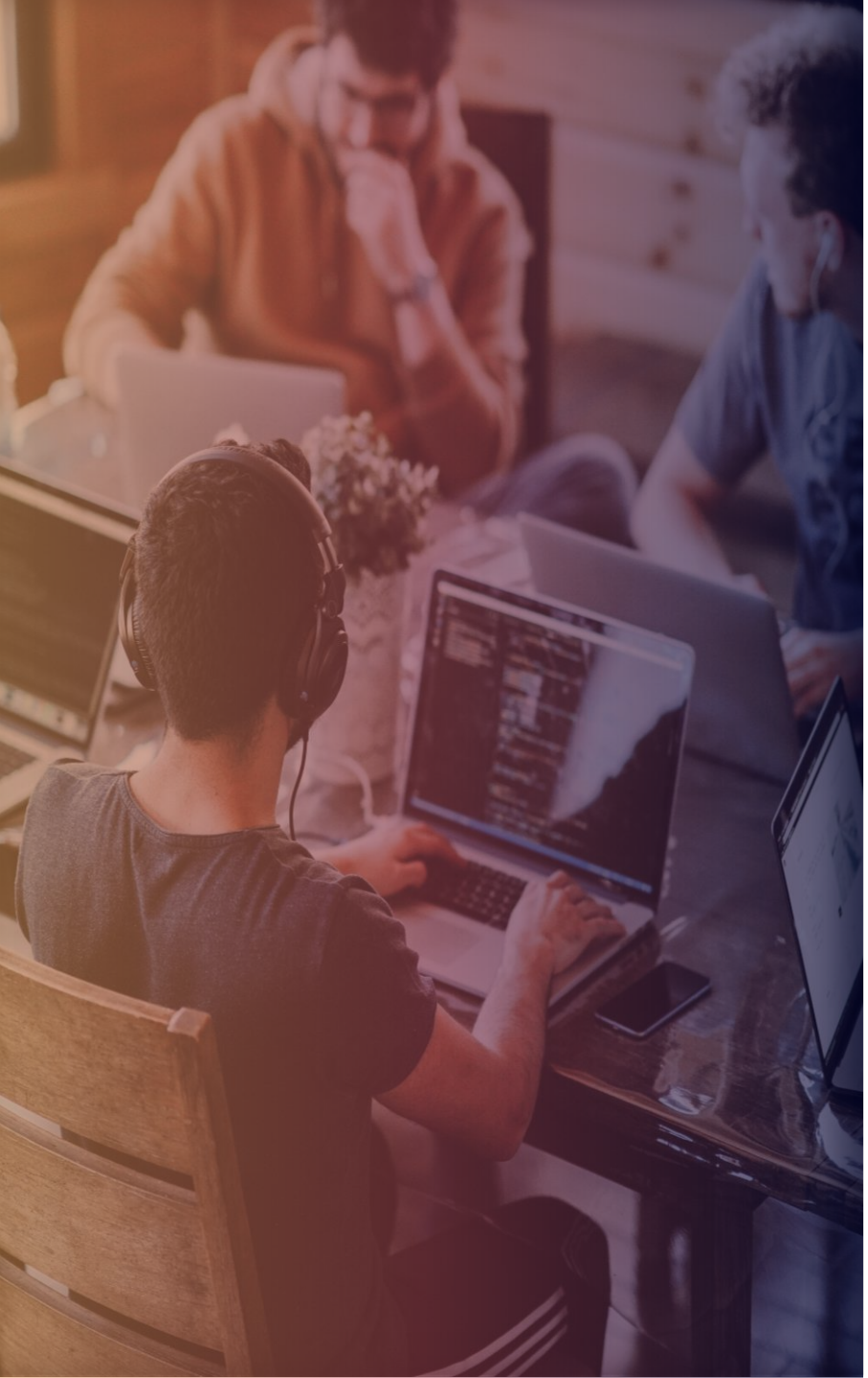
THE SECRET PANDEMIC

Cybercrime During COVID-19

PRESENTED BY:
LUKE HUTCHINSON, RPLU
GREG LYONS, AINS

ELITE SPECIALTY & WHOLESALE
Insurance Services

CA Insurance License 6000032



CYBERCRIME

The Secret COVID-19 Pandemic

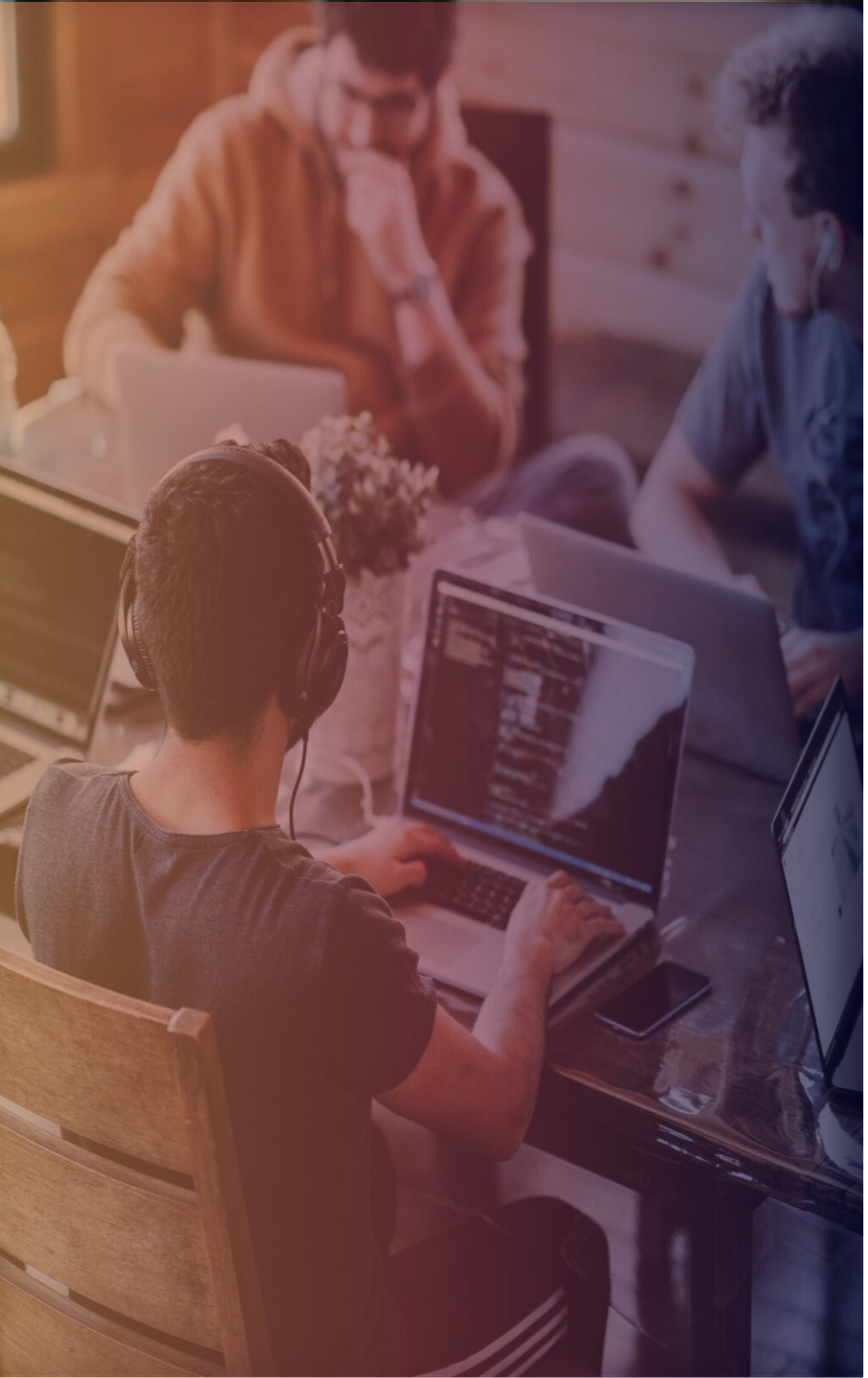
- Opportunistic & Sophisticated – Criminals are Prepared
- Spear Phishing's Newest Target: Senior Managers
- Clouds, Mobile Devices, VPN… Oh My! Corporate Security Newest Headaches
- Enterprise Ransomware
- Double Extortion
- Best Practices for Small Businesses

CYBERCRIME

The Secret COVID-19 Pandemic

Opportunistic & Sophisticated – Criminals are Prepared

- Utilizing software vulnerability scans, opportunistic hackers are looking for open doors & windows to target businesses with minimal security or known access points.
- Hackers have been laying dormant in systems for months or years to learn every detail about the IT department and internal security measures.
- Prior to attack, they are performing reconnaissance confirming company performance, current assets, and even searching for insurance policies to finalize the ransom amounts.



CYBERCRIME

The Secret COVID-19 Pandemic

Spear Phishing's Newest Target: Senior Managers

- Bad actors are targeting senior managers with access to bank accounts and who can authorize payments.
- Spear phishing campaigns, using employee info found easily on the dark web, focus on assistants to Senior Managers to bait them into clicking on links from trusted internal contacts.
- By targeting senior managers, criminals are able to access restricted information to be used in determining and executing ransomware.

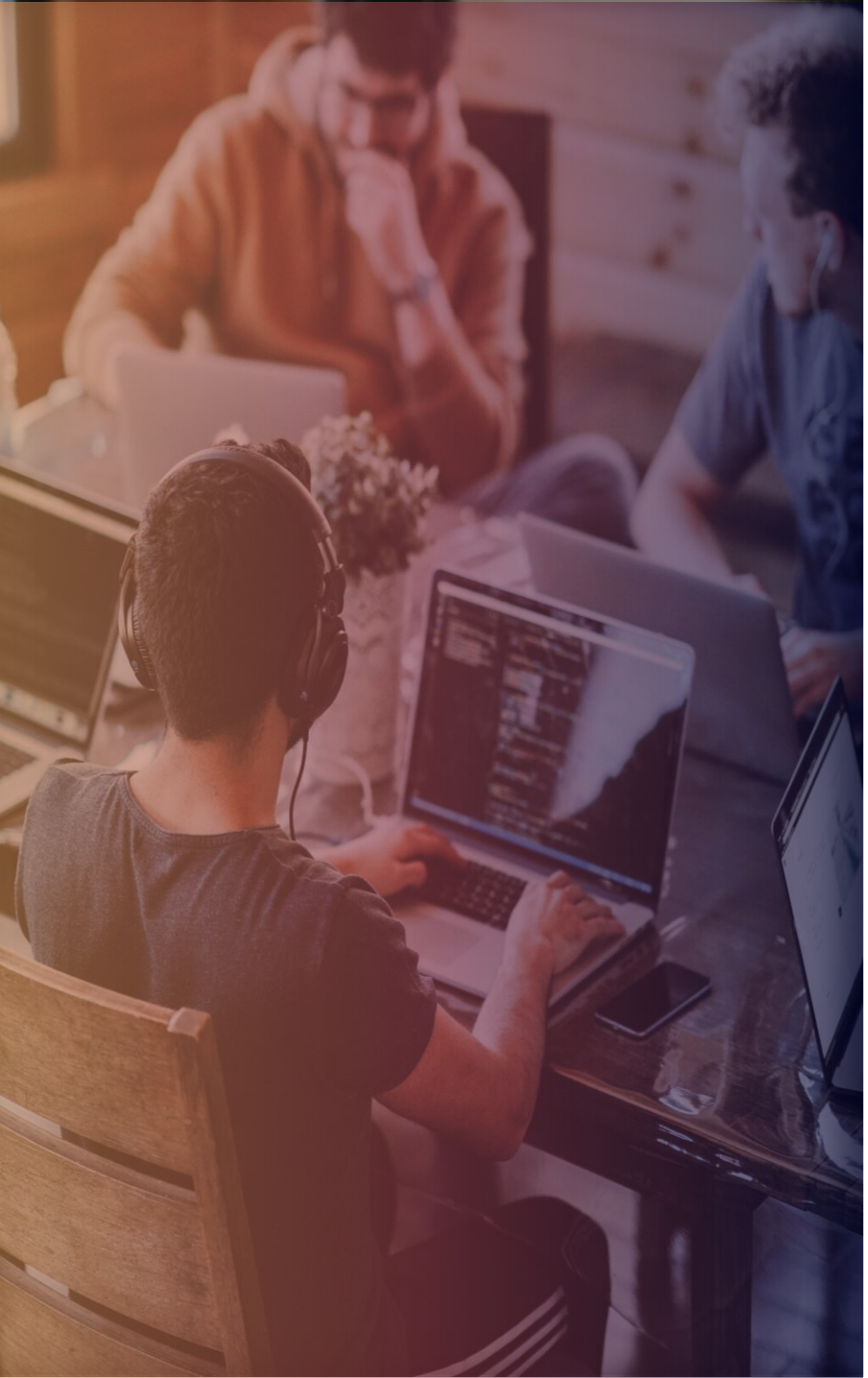

MOBILE DEVICES ARE QUICKLY BECOMING A TARGET ACCESS POINT FOR BAD ACTORS

CYBERCRIME

The Secret COVID-19 Pandemic

Corporate Security's Newest Headaches

- Cloud systems are not responsible for your data security including AWS & Google Cloud.
- As companies transitioned to remote work, VPN systems have been lagging in the scramble to keep employees up and running.
- Home computers are not as secure as systems in the corporate IT environment.
- Employees are more likely to click on malicious links when they are at home compared to being in the office.



CYBERCRIME

The Secret COVID-19 Pandemic

Enterprise Ransomware & Double Extortion

- According to CyberCube, Enterprise Ransomware is here to stay and likely to grow as an attack vector with accelerated growth in 2020 & 2021.
- Social engineering will be powered by artificial intelligence (AI) at scale. Cyber criminals will construct algorithms to hunt for individual targets and help them decide “which buttons to press” to make these targets act in a manner that suits the criminal.
- Double Extortion: if ransoms aren’t paid on time attackers will publish the business’ private data and screenshots of the systems that have been compromised on public websites.

CYBERCRIME

The Secret COVID-19 Pandemic

Criminals are Prepared – What about YOU?!

Businesses should consider:

- Providing regular, up-to-date training for staff on the latest online threats and trends in cybercrime.
- Using teaching drills and exercises with everyday scenarios that test employees' ability to detect scammers and respond appropriately to fraudulent requests.
- Training staff on the dangers of clicking on unsolicited email links and attachments and the need to stay alert for warning signs of fraudulent emails.
- Monitoring and protecting websites with an advanced website scanner, web application firewall to block cyberattacks, and installing updates immediately to repair vulnerabilities.
- Using a virtual private network (VPN) to be protected from all vulnerabilities when using any Wi-Fi network.
- Establishing a cyberattack response plan so employees are ready in the event of a breach.

THANK YOU

LUKE HUTCHINSON

(949) 550-6027

lhutchinson@elitespecialtywholesale.com

GREG LYONS

(949) 550-6026

glyons@elitespecialtywholesale.com

CA Insurance License 6000032