# WEBINAR: UNDERSTANDING CYBERSECURITY THREATS AND BEST PRACTICES

August 26, 2024

Special Guest:
Billy Steeghs, Co-Founder & Chief Operating Officer, OnDefend

Moderator:
Carrie King, Partner & Chief Compliance Officer, Ullmann Wealth Partners

ullmann wealth partners

OUR DISCIPLINE. YOUR FREEDOM.™

# BILLY STEEGHS
# CO-FOUNDER & COO
# ONDEFEND

Billy Steeghs brings over 25 years of IT engineering and cybersecurity expertise to his role as Co-Founder and COO at OnDefend, a Jacksonville-headquartered cybersecurity testing and consulting firm.

He specializes in crafting strategic cybersecurity services, solutions, and frameworks, focusing on preventative strategies and risk management.

OnDefend has become a beacon for innovation in cybersecurity solutions, integrating cutting-edge technology with practical strategies to ensure resilient and secure infrastructures.

Billy is dedicated to driving the evolution of cybersecurity practices to meet the dynamic challenges of today's digital landscape.

ullmann
wealth partners
OUR DISCIPLINE. YOUR FREEDOM.

# WHAT ARE SOME OF CURRENT CYBER THREATS?

- Ransomware: Cybercriminals use malicious software to lock up your data, demanding payment to restore access, impacting even small businesses.
- Supply Chain Attacks: Hackers target trusted vendors or partners to breach your network, making even small companies vulnerable.
- Zero-Day Vulnerabilities: Attackers exploit unknown software flaws before they're fixed, posing a serious risk to your business's security.

ullmann wealth partners

OUR DISCIPLINE. YOUR FREEDOM.

# WHAT ARE SOME BEST PRACTICES FOR AVOIDING SOCIAL ENGINEERING ATTACKS?

- Employee/Personal Training: Regularly educate yourself and your teams on recognizing phishing attempts and other social engineering tactics.
- Multi-Factor Authentication (MFA): Use MFA on all critical accounts to add an extra layer of security beyond just passwords.
- Secure Communication: Always verify requests, especially those involving sensitive information, through trusted and secure channels.

ullmann wealth partners

OUR DISCIPLINE. YOUR FREEDOM.™

# WHAT ARE SOME WI-FI BEST PRACTICES?

- Change Default Passwords: Immediately update default vendor and Wi-Fi passwords to something strong and unique.
- Avoid Public Wi-Fi for Sensitive Transactions: Use a VPN or avoid public Wi-Fi for important activities to prevent data interception.
- Create a Separate Guest Network: Set up a separate network for guests or smart devices to keep your main network more secure.

ullmann
wealth partners
OUR DISCIPLINE. YOUR FREEDOM.™

# WHAT ARE SOME ESSENTIAL CYBERSECURITY MUST-DOS?

- Keep Software/APPS Updated: Regularly update all software, including operating systems and apps, to protect against the latest security threats. (Computers, Servers, Phones, Tables, etc.)

- Use a Password Manager: Utilize a password manager to generate and store very long, unique passwords for all your accounts.

- Enable Multi-Factor Authentication (MFA): Enhance security by enabling MFA on all critical accounts. Including Social Platforms)

ullmann wealth partners

OUR DISCIPLINE. YOUR FREEDOM.™

# WHAT ARE BEST PRACTICES WHEN IT COMES TO COMPUTER MAINTENANCE?

- Regular Backups: Frequently back up your data to an external drive or cloud service to protect against data loss.
- Remove Unnecessary Files and Software: Periodically clean out unused files and uninstall software you no longer need to keep your computer running smoothly.
- Keep Security Settings and Software Updated: Ensure your firewall, antivirus, and other security settings are active and updated to the latest versions and patches to protect against threats.

# WHAT ARE SOME BEST PRACTICES TO PROTECT OURSELVES FROM TEXT SCAMS?

- Don't Click on Links: Avoid clicking on links or responding to texts from unknown or suspicious numbers.
- Verify the Source: If a text claims to be from a legitimate organization, contact them directly using a trusted method, rather than relying on the number or link provided in the text.
- Use Spam Filters: Enable spam filters on your phone to block and filter out potential scam texts automatically.

# WHAT SHOULD YOU DO IF YOUR IDENTITY IS COMPROMISED?

- Contact Financial Institutions: Immediately notify your bank, credit card companies, and other financial institutions to freeze accounts and prevent unauthorized transactions.

- Freeze Your Credit: Contact all major credit bureaus (Equifax, Experian, TransUnion) to freeze your credit and prevent new accounts from being opened in your name.

- Report the Theft: File a report with the Federal Trade Commission (FTC) and your local authorities to document the incident and begin the recovery process.

- Monitor and Update: Continuously monitor your credit reports and accounts for suspicious activity, and update passwords and security questions for all affected accounts.

ullmann wealth partners

OUR DISCIPLINE. YOUR FREEDOM.

# WHAT TO DO IF YOU HAVE BEEN HACKED?

YOU HAVE BEEN HACKED!

Here is a step-by-step guide of what you need to do.

- **Stay Calm:** It's natural to feel panicked, but staying calm is crucial. Take a deep breath and remind yourself that you can resolve this situation.
- **Disconnect from the Internet:** If you suspect your device has been compromised, disconnect it from the internet to prevent further damage. Unplug your Ethernet cable and turn off Wi-Fi on your device.
- **Secure Your Accounts:** Change the passwords for all your compromised accounts immediately. Use strong, unique passwords that include a combination of letters, numbers, and special characters. Enable two-factor authentication wherever possible.
- **Check for Unauthorized Access:** Review your accounts for any suspicious activities, such as unrecognized transactions or changes in personal information. Contact your bank or credit card company immediately if you notice any unauthorized transactions.
- **Inform Relevant Parties:** If your personal information, such as social security number or credit card details, has been compromised, inform the relevant authorities, such as your local police department and credit monitoring agencies.
- **Scan for Malware:** Run a full antivirus scan on your device to detect any malicious software. Use reputable antivirus software and ensure it is up to date. Remove any detected threats.
- **Update Your Software:** Make sure all your software, including the operating system, web browsers, and plugins, are up to date. Hackers often exploit vulnerabilities in outdated software, so keeping everything updated is crucial.
- **Enable Account Notifications:** Set up notifications for your accounts so that you receive alerts for any unusual activities. This way, you can take immediate action if any suspicious activity occurs.
- **Change Security Questions:** If your security questions have been compromised, change them immediately. Select unique questions and avoid using easily guessable answers.
- **Be Vigilant:** Stay vigilant and monitor your accounts regularly for any signs of suspicious activity. Avoid clicking on suspicious links or downloading files from unknown sources.
- **Educate Yourself:** Take the time to educate yourself about online security best practices. Stay informed about the latest threats and learn how to protect yourself from future attacks.
- **Consider Professional Help:** If you're unsure about how to handle the situation or suspect the breach is severe, consider seeking professional help from cybersecurity experts who can assist in securing your devices and accounts.

**Remember, being hacked is a stressful experience, but by following these steps, you can minimize the damage and regain control of your digital life. If you have any questions, please contact us.**

OUR DISCIPLINE. YOUR FREEDOM.™

1540 THE GREENS WAY, JACKSONVILLE BEACH, FL 32250 • (904) 280-3700

ULLMANNWEALTHPARTNERS.COM ULLMANNWEALTHPARTNERS

ullmann wealth partners

- Stay Calm
- Disconnect from the Internet
- Secure Your Accounts
- Check for Unauthorized Access
- Inform Relevant Parties
- Scan for Malware
- Update Your Software
- Enable Account Notification
- Change Security Questions
- Be Vigilant
- Educate Yourself
- Consider Professional IT Help

ullmann wealth partners

OUR DISCIPLINE. YOUR FREEDOM.™