|skät| |är| |'dāvis|

Scott R. Davis

Cyber Security Professional | MSP Coach | Public Speaker

Scott is an innovative senior technology professional with over twenty years in leading IT infrastructure and network security compliance for organizations of all sizes. serves as the Senior Sales Engineer with Liongard, bringing his in-depth knowledge of multi-year business planning, cybersecurity planning, technology documentation, workflow design, project management, and network design to MSPs around the globe. Scott is an active member on the Security and Compliance team with Liongard. Scott's background and knowledge of PCI-DSS, HIPAA, NIST, GDPR, CCPA and other state breach notification laws allows Scott the ability to quickly identify and develop a plan to bring organizations to compliance. In addition to being part of Liongard, Scott is an adjunct professor at Harrisburg University and NuPaths, produces a weekly video podcast called The Morning Breach, and is the President of the Cybersecurity Association of Pennsylvania.

As Seen At:

CBS 21 · FOX43 EXPECT MORE · PA PENNLIVE Patriot-News · ITNATION SECURE · MSP insights · NGTV · CHANNELe2e from entrepreneur to exit

FOR BOOKING VISIT SCOTTRDAVIS.COM

@scottrdavistech · @ScottRDavis · @scottrdavispa · @scott-r-davis

|skät| |är| |'dāvis|

Scott R. Davis

Speaking Topics

- Social Engineering & Phishing
- MSP Onboarding Process
- MSP Security Sales with Compliance
- Upgarde your Technical Documentation
- Getting Started In Cyber Security
- Cyber Security Annual Training
- Future of Cyber Security
- Teaching Kids Cyber Security
- IoT Risks and Securing your home
- Change Management

and more ...

Socialize eTrepid
Public Relations & Marketing Consultant at eTrepid, Inc.
September 27, 2021, Socialize worked with Scott R but at different companies

We are exceptionally pleased with the presentation Scott Davis presented to our viewers during our Coffee and Conversation Webinar. Scott focused on Change Management. He was well knowledgeable, engaged, and enthusiastic during the event. We recommend Scott Davis when you need someone to discuss technology and or IT for your viewers.

Michelle Mathason Brown
Recycling Manager at LCSWMA
May 27, 2020, Michelle worked with Scott R but at different companies

I had the pleasure of attending the panel on Cyber Security for the Solid Waste Management Industry at the 2019 PROP Conference, in which Scott shared his expertise in recovering after a cyber attack. His deep knowledge of the physical, digital, and human vulnerabilities in the industry's processes and procedures was impressive and illuminating. His wisdom on cybersecurity is clearly driven by a sincere desire to help his clients succeed in preventing or recovering from the worst possible scenarios.

The Evolution of Social Engineering and Phishing

Audience:

Cyber Security Professionals, Technicians, Business Owners, End Users

Presentation Summary

Today's phishing and social engineering campaigns are successfully gaining the trust of end users by utilizing emotions. Once a scammer can unlock the emotions of a user, the data they aim to collect is as good as theirs.

Emotions are often left out and not discussed during cyber security training sessions. Yet during 2020, the emotional desire to learn more about the pandemic lowered end users risk detections and they clicked and opened files in record numbers in the hopes of learning the latest news. Successful usage of these emotions can generate that false sense of security or urgency that scammers need to capture the desired data to collect a payout.

Social engineering is not new and has been around long before the internet or the need of people to store pins or passcodes. What we see now is that users have more useful data readily available as our devices have become an extension into our lives, and sometimes even our memory bank. Gaining the credentials to bank accounts, social networks, personal computers, and even corporate networks all lead to measurable successes which often times started with a that social engineering campaign.

Today's presentation is going to trigger an array of your emotions, so you can see and feel how scammers have mastered this artform in order to be successful in accessing and capturing your data.

Come prepared to leave the presentation and reimagine how you are training your own staff as well as the end users on how to spot these harder to detect social engineering attacks.

Purpose

The mis-spelled and easy to spot phishing attacks are dying. Replacing those are well thought out, researched, and artfully designed campaigns which target your emotions. Targeting emotions to reduce the user's security concerns often leads to a high rate of success for the attacker. The purpose of this presentation is to highlight and share the latest artform of social engineering so that proper training can be implemented for your staff and the end users that trust you to keep them safe and secure.

|skät| |är| |'dāvis|
Scott R. Davis

How to dominate your onboarding process

Audience:

MSPs, MSSPs, IT Vendors, VARs
Owners and Onboarding Leads

Presentation Summary

The client onboarding is the first impression that each end user will have of your MSP. Often times identifying and winning over the most challenging of end users starts with onboarding, and the last thing you want or need is that one end user that never forgets that negative first impression. So, are you setting a standard of excellence or simply checking the boxes?

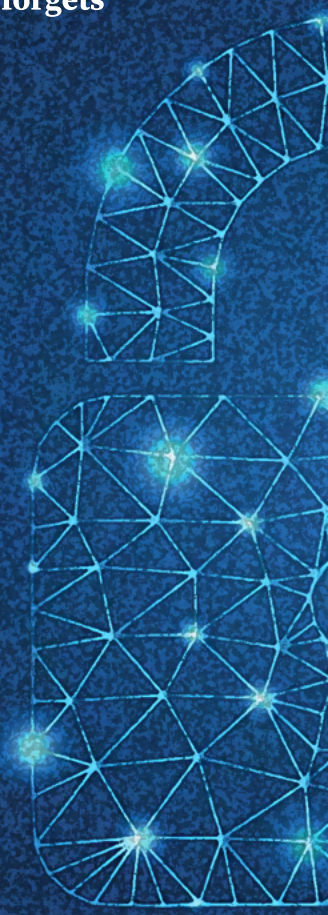
This presentation will walk you through how you should position your onboarding process to leave the right first impression and win the support of every user out of the gate. You will not only learn the process but leave with the tips and tools needed to start evolving your onboarding today.

The onboarding process begins before your take the first support call, understanding and building the documentation of a client takes time and during this time your focus should be on ensuring the I's are dotted and T's crossed. Transitioning services and tools from one vendor to another involves unique processes and will pose challenges that could leave an end user less than satisfied.

Completing the onboarding with a report deliverable will allow you to close the onboarding and ensure your newest client is now aligned and has a plan to conforming to your best practice requirements.

Once you've mastered the process and the tools used to conquer the onboarding process, it's time to optimize, so you're no longer sending the higher paid technicians onsite to evaluate and audit your new client.

So, if you know you need to improve the process or think you can do it better, this presentation is a must attend.



Purpose

Being a part of hundreds of onboarding's and offboarding's, Scott R. Davis was instrumental in drafting and creating a unique process of welcoming new partners and their users to managed services. Leaving the first impression that they are in the right hands, and we are here to work with each end user as needed. Join Scott as he will walk through his proven process from start to finish leaving the attendees with the tools needed to improve their own process.

|skät| |är| |'dāvis|
Scott R. Davis

Don't Trust Me – Weighing Zero Trust with the demand for more access.

Audience:

MSP, MSSP, IT Vendors, Business Owners, Internal IT Departments

Presentation Summary

I've never met an end user that wanted less permission than they were provided. Even worse, I rarely run into IT people that feel they have too much access. The concept and design of Zero Trust is to never trust and always verify, yet too often we find ourselves battling out what a user thinks they need and what they actually need.

When designing today's network infrastructure, a zero trust model must be adopted in some fashion. After all, you wouldn't want to connect to my access point, which just happens to be sharing the same SSID as the one maintained by your business. If you're not considering adopting at least some form of zero trust, then the network is already at risk.

In today's presentation we will review the fundamentals like disabling network ports that are not actively being used to disabling the wireless infrastructure when your office is closed. Our journey will move to explore the bigger threats like applications that still require local admin rights and identifying who has access to what.

Zero trust isn't and shouldn't be seen as rocket science, and the goal of this presentation is to present a baseline that you can achieve in a short time period to begin your own journey of providing better security for your customers and ultimately even better protecting your own office.

Purpose

The purpose of this presentation is to help service providers understand that starting their journey to securing their clients with zero trust can be easier than they think. Using a limited slide deck and amazing story telling, Scott R. Davis will build trust and provide the attendees with the tools and concepts to start implementing zero trust for their clients and their own offices today.

|skät| |är| |'dāvis|
Scott R. Davis

How Compliance should be driving your security services

Audience:

MSP, MSSP, IT Vendors Owners and Sales

Presentation Summary

Compliance requirements are changing almost daily, understanding the core ones can help you improve your client's technology security portfolio. This presentation is going to help you position the already known fundamentals with the compliance requirements to push a security first mentality to your clients.

Managed Service Providers (MSP) within the United States have state, federal, industry, international, and sometimes even local security compliance requirements they must follow. The trend of when and how cyber incidents have to be reported is rapidly evolving and soon may be the foundation for identifying the risk and acceptance of cyber security insurance policies.

Understanding the baseline of PCI-DSS allows you to place a foundation of security requirements for probably 95% of your client base. Your MSP is already addressing many of the core-requirements, but often times you are not communicating that to the customer.

This presentation is designed to walk you through the core security practices you are already doing and introduce the logical next steps to take, to bring clients into compliance with PCI-DSS, HIPAA, CIS, and others.

Now that you understand the basics of compliance requirements your clients face, you'll be able to improve the security for your end users and your own MSP.

Purpose

The purpose of this presentation is to highlight how aligning compliance requirements to your stack will allow your MSP to scale and improve overall security from the end users to your back office.

|skät| |är| |'dāvis|
Scott R. Davis