VINCENT SCOTT

https://cincinnaticommissioning.org/

Vince is a retired Navy Cryptologist/Information Warfare Officer and serial entrepreneur who has started two companies, two not for profits, and is passionate about cyber defense. On active duty he was deployed 8 times including the first Gulf War, Bosnia, Afghanistan, and Iraq. He currently serves as the CEO of Defense Cybersecurity Group, a cyber consulting company focused on the cyber requirements for the Defense Industrial Base where he brings the cyber offensive mindset of his Navy career to cyber defense for US companies. He also serves as Deputy Chief of the FBI Infragard Defense Industrial Base sector

TIP 1. YOU'RE NOT TOO SMALL TO BE A TARGET

I once had a person in a major corporation say to me: "We are a soap and diaper company. Who would hack us?" My answer: "Everyone who wants a piece of your $85 billion a year." Clearly a huge example, but it scales all the way down. Who would hack you? People who want your money. People who want your IP. You are not too small to be a target, and you live in an incredibly dangerous neighbourhood. The miracle of the internet is that you are only one address away from the most ruthless and capable criminals. Act like it.

TIP 2. GUARD YOUR BANK TRANSFERS VERY CLOSELY

Bank transfers rather than cheques are becoming increasingly common. Guard your bank transfer information. View ANY email requesting a change in bank transfer information with extreme scepticism. Even if it looks perfectly legit, pick up the phone, and dial a number you know (not from the suspect email), and verify that it is legit. Every time. Complex scams around this are standard attacks against small business. Don't fall for it.

TIP 3. ENGAGE TWO-FACTOR EVERYWHERE YOU CAN

….but especially banking. Nearly all banking, and many other platforms, offer two-factor authentication now. Yes, it is a little less convenient. Always put 2FA on your bank accounts and your primary email accounts. Always always always.

TIP 4. PEOPLE ARE MORE IMPORTANT THAN HARDWARE

The US Special Forces have four truths that they go by. This is #1 and it applies here too. When we think about cybersecurity we tend to think about technology and technology answers. Buy the new cool tool! Get the AI! That will protect me. The actions and capabilities of your people are way more important than how cool your tools are. Thousands of companies every day are paying licensing fees on tools they think are protecting them but, in reality, are effectively sitting on the shelf because no one is using them. There is very little fire-and-forget in this business. If you want to improve your cybersecurity: up skill your people. This means training people to, for example, guard your bank transfer information. It also means that when you grow and want to up your game, then think about hiring the right people first. You will be fabulously better protected if you hire the right person and have them use free tools, than buying expensive tools that no one knows how to use. I am continuously astonished at how often I see companies making the second choice.

TIP 5. HIRE AN IT SERVICE PROVIDER THAT HAS A SECURITY MINDSET

Most small businesses hire someone else to do their IT. These companies fall under the general rubric of Managed Service Providers or MSPs. All MSPs are not created equal and many are not security conscious. Choose wisely.

TIP 6. HOLD YOUR IT SERVICE PROVIDER ACCOUNTABLE

Once you have chosen wisely realise they must be held accountable for providing good services by someone inside your organisation. They are not fire-and-forget either. My experience with security and MSPs is that you have to engage with them regularly or security falls off. You hear nothing and so presume all is good. That is not necessarily the case for security. Everyone knows when email falls over, but you might be hearing nothing on security because all the guards are asleep. My experience is that they will fall asleep unless you check those guards periodically.

TIP 7. SCALE CYBERSECURITY WITH YOUR BUSINESS

As you grow - your risk rises, and your cybersecurity should scale with that. As a micro business, you are pretty limited in what you can do. As you grow though, you should add in additional protection. Engaging the right people first but then creating and maintaining a more sophisticated cybersecurity capability. I see many companies that have grown to medium and large enterprises who are still not putting additional security capabilities in place. That works until it doesn't; but then the consequences can be quite severe.

TIP 8. USE LONG PASSWORDS; TRY THE PASSPHRASE

There is a lot of focus on complexity of passwords. Substituting 3s for Es for example. The bad guys know those tricks too and build them into their password crackers. The best protection are longer passwords or passphrases. Use passwords at least 14 characters long for your important accounts. Banking? Super long. Your login to the Wall street Journal perhaps does not matter so much. While you are at it - avoid password re-use, especially on critical accounts.

TIP 9. KNOW WHAT INFORMATION YOU NEED TO PROTECT

Finances are the obvious starting point, but what about other things? Are you inventing that next cool device? Are you supporting your military's operations? What needs to be protected? Then focus your efforts on those things.

TIP 10. HAVE A PLAN FOR WHEN BAD THINGS HAPPEN

Bad things will happen. Have an Incident Response Plan. For micro companies, this might be ad-hoc, but as you scale up, this should rapidly become more robust. As more government agencies mandate reporting, you should know who you have to report to and when, you should be aware of the free resources out there to help, and if you are going to bring in experts who they are and who makes the decision to call.