Schedule a Workout Session with a Business Cyber Security Coach

Your day starts with an energy bar and a three-mile run. But on your laptop awaits a long list of business cyber security notifications that require your immediate attention. You rush to get through the alerts before others sign in and you're swamped with the usual fire drills.

And that project you've been trying to get to for the last five weeks? Well, it's just going to have to wait for another day.

Wouldn't it be great if you could get this all into shape through a workout session with an expert business cyber security coach?

> *Someone who could run you through a workout program of security solutions to keep your network healthy, provide the visibility you need, and get you back to working on other priorities!*

Until we arrange that for you, here are a few items to consider—three of the most common cyber security threats you face with security best practices to keep them off your emergency response list. Plus, we've listed cyber-security solutions that simplify your life while reducing the risk of a vitality-draining breach.

Weak or Stolen Passwords

According to Verizon, 81% of recent hacking-related breaches leveraged weak or stolen passwords. Thus, the time for sticky notes on monitors preserving passwords like John1987 are far in the past. Your employees need secure passwords that can be managed safely.

How are you ensuring that passwords aren't putting your business at risk from a breach?

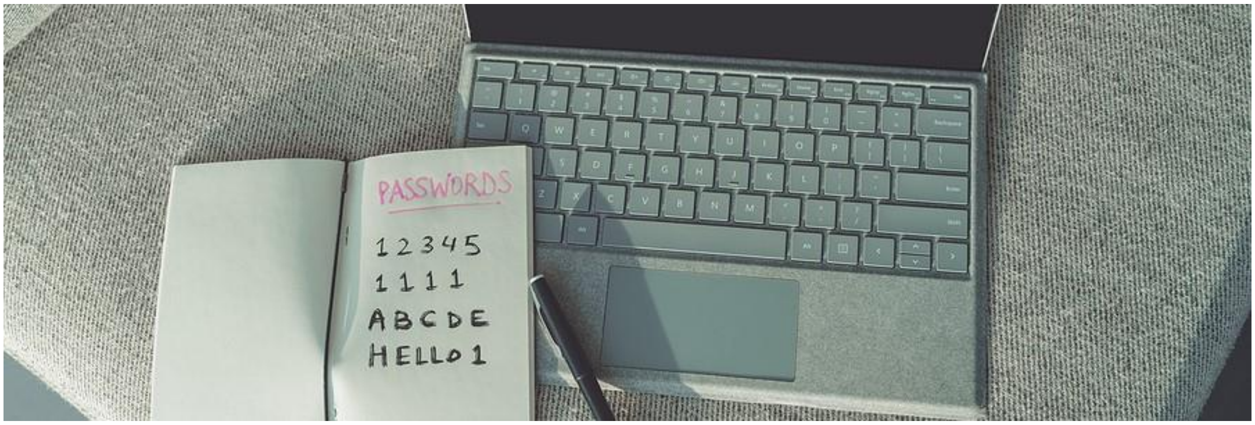
Password Best Practices

To start with, it pays to be password **SMART:**

- ✓ **S**ymbols, letters & numbers
- ✓ **M**ore than 12 characters
- ✓ **A**void personal information
- ✓ **R**efuse to reuse old passwords
- ✓ **T**rust password management tools

Multi-Factor Authentication

Multi-factor authentication (MFA) tools provide additional proof of identity beyond simple passwords. They require a user to not only authenticate with something they know, such as a password, but with something they have or something they are as well. This limits a cyber criminal's ability to use stolen credentials to access accounts.



Forgotten Passwords

Employees today awkwardly manage a plethora of passwords—191 in fact for the average business employee. Furthermore, they dutifully authenticate to websites and applications over 150 times per month. Overall, the average 250-employee company counts almost 48,000 passwords in use.

No wonder your employees are constantly forgetting their passwords and asking for a reset!

Password Storage and Management Tools

Password management tools make it possible for users to leverage strong passwords without having to remember them all. Users also set up reminders for when passwords need to be changed.

By adding MFA solutions and offering users easy access to an identity portal, users only need to log in once. Hence, they are no longer required to remember multiple passwords.

WatchGuard AuthPoint

WatchGuard Technology's unique multi-factor authentication solution helps to minimize the risk arising from lost or stolen credentials. Thus, the likelihood of network disruptions and data breaches shrinks to manageable size.

> *WatchGuard delivers this solution entirely from the cloud for easy set-up and management even with limited staff.*

AuthPoint goes beyond traditional two-factor authentication (2FA) by considering innovative ways to positively identify users. For example, its Mobile Device DNA approach works easily for everyone with a smartphone.

Even better, AuthPoint's users authenticate just once to cloud applications. After sign-in, they are granted access to all the Cloud applications and resources they need to do their work.

Willing Clickers

According to Digital Guardian, 91% of cyber-attacks start with a phishing email. As long as organizations have willing employees that click on the link, hackers will continue to leverage and evolve this method for malware delivery.

Phishing education is an important way to ensure that all your employees know the warning signs of a phishing attempt. But you need phishing protection in place as well.

You need a solution that provides protection and offers an education refresh.

Phishing Education

Education is critical for helping users know the risks of phishing emails and the warning signs. You want to ensure that your employees are prepared to defend themselves against anything that comes through their inbox.

DNS Monitoring and Blocking

Education alone can't completely protect your employees. As phishing emails become more personalized and targeted, it is just a matter of time before something gets clicked. You need to have a solution in place that monitors DNS traffic and blocks access to malicious sites.

DNSWatch

eMazzanti's eCare Secure Route detects malicious DNS requests and blocks access to these sites. These events become teaching moments for your employees. They function as an effective way to engage people about the risks of clicking on phishing links.

Schedule a Business Cyber Security Workout Session

Now, about that security workout session. eMazzanti has trained, certified, and experienced business cyber-security experts ready to customize a cyber-security program for your business. Having earned WatchGuard Partner of the Year 5X, they know their business cyber security. Call today to schedule a free consultation.