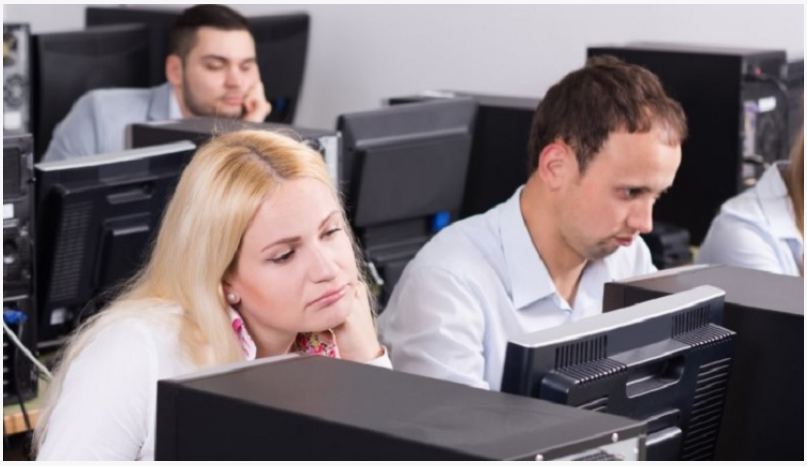
# Security fatigue is real: Here's how to overcome it



DUBAI, UNITED ARAB EMIRATES, November 24, 2022 / EINPresswire.com/ -- Do your employees take more risks with valuable data because they've become desensitized to security guidance? Spot the symptoms before it's too late, explains Phil Muncaster, guest writer from ESET

IT security is often regarded as the "Department of No" and sometimes it's easy to see why. In a world of escalating cyber-risk, expanding attack surfaces and a fast-growing cybercrime economy, security teams are understandably keen to limit the damage their employees could cause. After all, it takes just one misplaced click to unleash a potentially devastating ransomware compromise. But when the burden on employees becomes too high, they may react in unexpected ways, which actually increases cyber-risk in the organization.

This is known as "security fatigue" and it in a worst-case scenario it can lead to reckless and impulsive behavior – quite the opposite of what IT teams want. To tackle it, security needs to work more seamlessly, limiting the number of decisions users need to make and rebalancing protection and productivity for a world of hybrid working.

What is security fatigue and how bad is it?
Humans are often thought of as the weakest link in the corporate security chain. That's why IT security departments are so keen to mitigate the risk from (not just) negligent insiders. On the one hand, they're right to. An estimated 67% of companies experienced between 21 and over 40 insider incidents in 2021, up from 60% in 2020 and costing them an average of over US$15m to remediate.

However, when staff feel bombarded by security warnings, policy rules and procedures at work, and media stories of breaches and threats in their spare time, a state of exhaustion may set in. This security fatigue is characterized by a feeling of helplessness and loss of control. Individuals

may find it all so overwhelming that they retreat from corporate policy and go their own way. There may also be a sense of resignation: that breaches are going to happen whatever they do, so they might as well ignore all those stressful security alerts.

It's more common than you might think. A 2018 study revealed that over half (55%) of EMEA employees are not regularly thinking about cybersecurity, and nearly a fifth (17%) aren't concerned about it at all. Evidence suggests that younger staff are even more prone to become fatigued by excessive security demands.

What are the top symptoms of security fatigue?
Unfortunately, this could have a seriously destabilizing impact on corporate security. Among the tell-tale signs of security fatigue are employees who:
Take more risks with phishing emails, perhaps deciding to click through on links or open attachments out of interest.
Practice poor password management, such as reusing weak credentials across multiple accounts. According to one recent study, 43% of employees admit to sharing logins and even avoiding their work altogether to reduce the stress of logging in.
• Log-in to corporate networks without a VPN, although this may be restricted in some organizations.
• Use unsecured public Wi-Fi hotspots when out and about to log-in to sensitive corporate accounts.
• Fail to update their devices and machines regularly. A new EY study claims Gen Z and Gen Y employees are far more likely than older colleagues to disregard mandatory patches for as long as possible.
• Fail to report incidents immediately to superiors or the IT department. The same EY study reveals that nearly a fifth (16%) of employees would try to handle a suspected breach by themselves, rather than notify someone else.
• Use work devices for personal use, including risky activities such as internet downloads, gaming and online shopping. One study claims that half of employees now see their work device as their personal property.
• Circumvent security in other ways: Another report reveals that 31% of office workers aged 18-24 have tried to bypass policy.

How to tackle security fatigue
The rapid shift to mass home working in 2020 triggered a knee-jerk response in many organizations as IT teams sought to limit their risk exposure by placing onerous new rules on their employees. Now the hybrid workplace is beginning to emerge from the ashes of the pandemic, there's an opportunity to revisit these restrictions, with an eye on reducing the risk of security fatigue.

Consider the following:
• Listen to your end-users to better understand how security impacts workflows and disrupts productivity. Try to design policies that better balance the needs of employees with the need to

minimize cyber risk.
• Limit the number of security decisions users need to make. That could mean automatic software patching, remote security software installation and management of laptops and devices. And running detection and response services in the background to catch and contain threats when they breach network defenses.
• Support enhanced log-in security while minimizing effort, with password managers, biometric-based two-factor authentication and single sign-on (SSO).
• Limit the number of security related messages you bombard users with. Less is more.
• Make security awareness training more fun, via shorter sessions (10-15 minutes) that use real-world simulations and gamification, to change behavior.

For security to work effectively, you need to create a culture where every employee understands the crucial role they play in keeping the organization safe, and proactively wants to play their part. That kind of culture can take time to build. But it starts with understanding and tackling the causes of security fatigue.

Sanjeev Kant
Vistar Communications
+971 55 972 4623
email us here

---