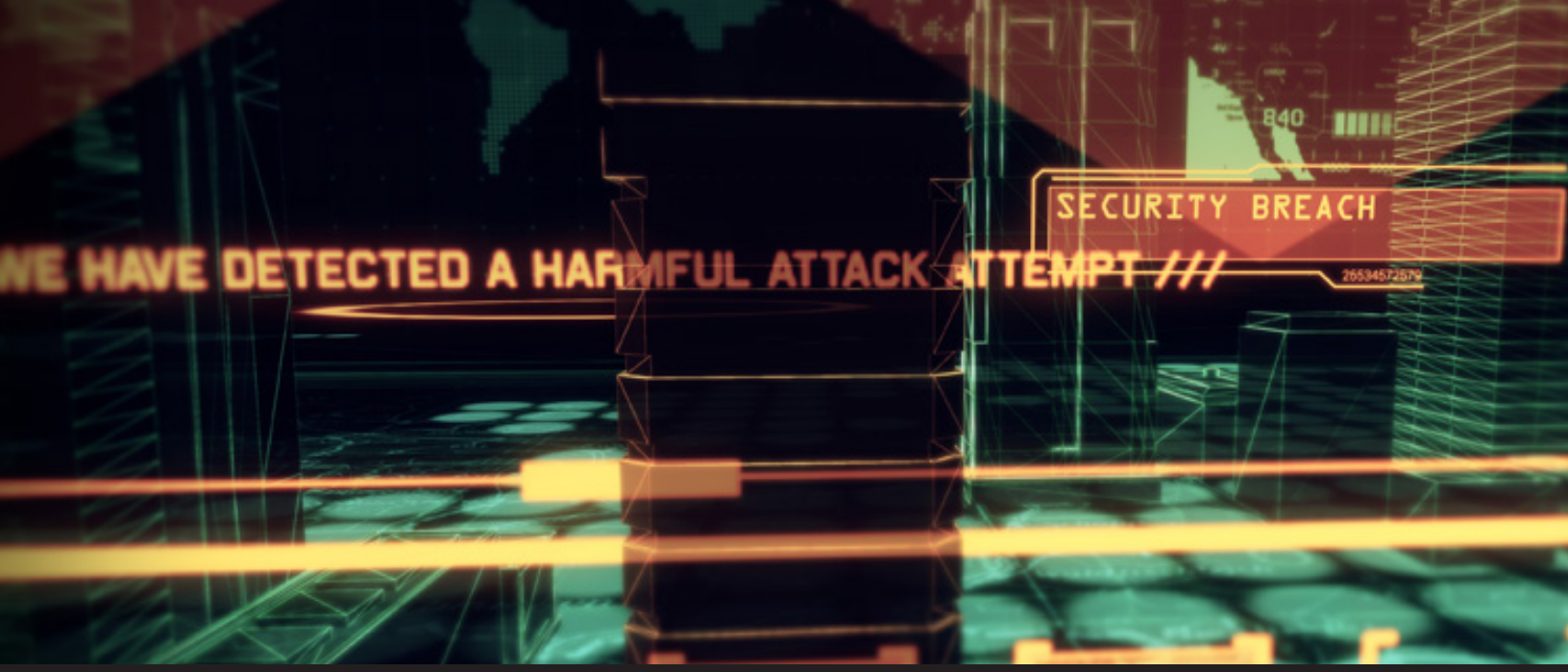

Are Your End Users Suffering from Security Fatigue?

Devolutions

THESE DAYS, IT SEEMS LIKE MASSIVE DATA BREACHES ARE MAKING THE HEADLINES ALMOST EVERY DAY.

These days, it seems like massive data breaches are making the headlines almost every day. And it's not just big enterprises that are getting hit. Small and midsize businesses (SMBs) have become "Ground Zero" for cyber crime.

The Enemy Within

We all know that System Administrators, Network Administrators, SecOps and other **IT pros are overwhelmed by a constantly growing list of security-related tasks**, such as implementing password policies and best practices. However, they are fighting a second battle on another front, and against a totally unexpected enemy: end users!

Indeed, end users have always been (and always will be) the weakest link in the IT security chain. But this vulnerability is made even worse by a condition called "security fatigue."

What Is Security Fatigue?

The National Institute of Standards and Technology (NIST) **describes security fatigue as, "a weariness or reluctance to deal with computer security."** Here are some of the symptoms:

- **End users cut corners and do things the easy way** by storing passwords in their browser, choosing weak passwords, or storing passwords in spreadsheets, on sticky notes, etc.
- End users **immediately click on all links and attachments, without first confirming that they're legitimate and safe** — which is how spear-phishing attacks take root.

Curing Security Fatigue

Security fatigue is a growing problem and a major concern for IT professionals who are fed up with telling end users not to put the organization at risk! The good news is that there are some ways to cure (or at least alleviate) security fatigue. Here are some suggestions:

1. **Use a centralized password management tool** that forces end users to create strong passwords.
2. **Implement a Privileged Access Management solution** like Devolutions Server (DVLS) that is powerful, yet simple and easy to use.
3. Make it as easy and painless as possible for end users to install software updates.
4. Let employees securely store their personal data and teach them how to safely shop online at home. **Both of these help boost their security awareness and alertness.**
5. **Communicate, communicate and communicate!** As advised by information-age.com: "It is vital that end users have a full understanding of the most common ways for threat actors to target them. This includes educating employees that they will be targeted, encouraging them to be vigilant at all times, teaching employees what qualifies as sensitive data, how to identify and avoid threats, acceptable use policies and security policies.

What's Your Advice?

As an IT pro, you're already using several security tools to fortify your cyber defenses. But you also know that security fatigue among end users can create gaps and vulnerabilities. **What are some of the ways you've dealt with this in your organization?** Please comment below by sharing what works, and just as importantly, what doesn't!