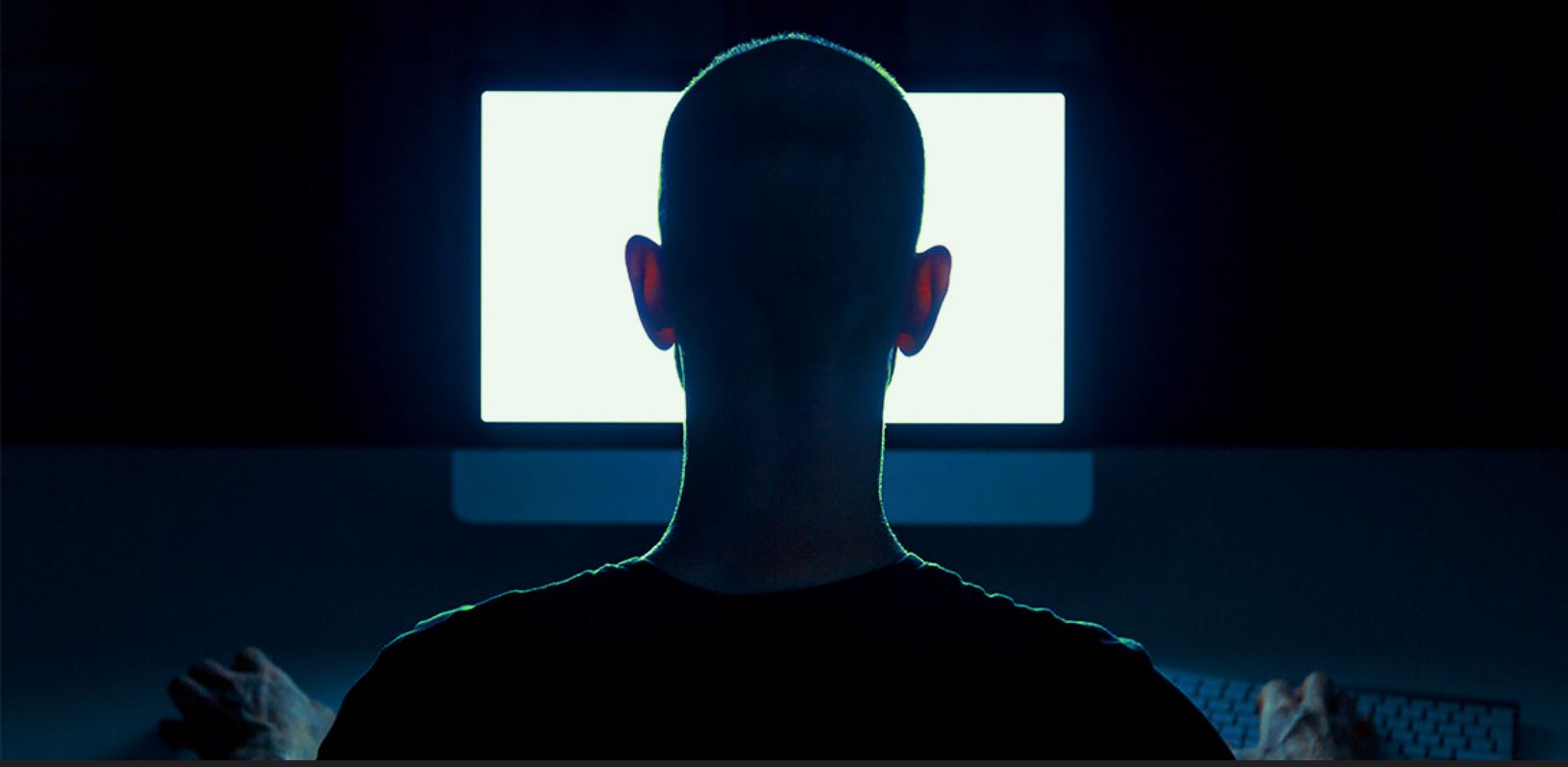

Surveys Reveal the #1 Fear of IT Pros

Devolutions

A SURVEY REVEALED THAT MISTAKES BY EMPLOYEES WAS THE TOP CORPORATE RISK TO SENSITIVE DATA.

It's not that the corporate Powers That Be will enforce a dress code (since when is a t-shirt that says "I went outside once but the graphics weren't very good" not formal?!). It's not the possibility of Dr. Who getting cancelled (who wants to live in a universe without a TARDIS?). And it's not getting stuck in an elevator with people who get their Star Wars, Star Trek, and Lord of the Rings details mixed-up ("my favorite scene was when Frodo took the U.S.S. Enterprise to destroy Death Star!").

No, according to a survey [PDF] by to SaaS vendor BetterCloud, the number one fear among IT pros is well-meaning but negligent end users. And if that wasn't damning enough, a separate survey of IT pros commissioned by encryption hardware vendor nCipher revealed that mistakes by employees was the top corporate risk to sensitive data.

So, if you're an IT pro and you can't shake the feeling that the biggest threat to your peace of mind — and maybe to your job — is the generally friendly men and women who roam the halls with you, then you're not alone. And if you're a non-technical end user reading this, I'm afraid your suspicions are true: IT thinks that you're the enemy, because unfortunately, in many cases, you are.

First, the Bad News...

Here are just some of the tragic things that some end users unwittingly do:

- Store passwords in their browser, in spreadsheets or in text files.
- Use the same password everywhere.
- Choose weak passwords.
- Fall for spear phishing emails and texts.
- Insecurely share passwords with colleagues (and almost always without authorization to do so).
- Fall for various online scams at home that put their personal device — and potentially the corporate network — at risk.

Now for Some Good News!

If your end users are unintentionally part of the security problem instead of being part of the solution, the good news is that you can be proactive and mitigate the potential damage. **Here are some suggestions:**

1. Implement a Principle of Least Privilege (POLP) policy and Zero-Trust Architecture.
2. Deploy a centralized password management tool like Devolutions Password Hub (DPH) that locks down password security, yet is simple and intuitive for end users.
3. Implement a PAM solution like Devolutions Server (DVLS) to control and monitor access to sensitive assets and privileged accounts.
4. If you cannot centralize device management, then make it as easy and painless as possible for end users to install software updates.
5. Recognize when your end users are suffering from "security fatigue", and provide them with training and resources so they can go from security zombie to superhero (so they can stop keeping you awake at night!)

Your Take

If you're an IT pro: Are well-meaning but negligent end users your number one fear? If so, please share some of your top concerns (read: nightmares). If your end users are compliant, then please share what you find even more worrisome. Ransomware, maybe?

If you're an end user: What do you want IT pros around the world to know about your situation? Share what you need and how you want to be treated. Are you fed up with being seen as one of the bad guys? Or do you understand where IT is coming from and sympathize with their challenges?