As an MSP, you do everything you can to protect your clients. But at the end of the day … end users are still wild cards. All it takes is one click on the wrong email and you have a cybersecurity mess on your hands.

That *almost* happened to Paradigm Technologies. But SaaS Alerts saved the day — and reminded their customer, a healthcare organization, just how valuable Paradigm is.

The first part of this story will sound familiar: an end user at the organization opened a phishing email. *(Uh oh.)* Then they entered their Microsoft username and password. *(Double uh oh.)* And the coup de grace: they even typed in their MFA code. *(Triple uh oh!!)*

Luckily for the organization, Paradigm uses SaaS Alerts to cover their clients' SaaS.

The hacking attempt came from overseas, which triggered a geolocation alert. Shortly after, the Respond module's automated remediation tools shut down the attack.

"SaaS Alerts paid for itself with just that one catch," said Gary Fisk, owner of Paradigm Technologies.

As a healthcare organization, the client's risk for sensitive data exposure and ransomware is especially high. So the end user who accidentally gave up their credentials wasn't exactly *thrilled* to learn they had single-handedly almost caused a catastrophe.

Still, they were relieved that SaaS Alerts let them off the hook. And it became even more obvious that Paradigm's services are worth every penny.

As an added bonus, the incident "reignited the fire" for the organization to get serious about cybersecurity training. Paradigm has since rolled out more awareness trainings to teach end users about phishing red flags — *and when not to click that funny-looking link.*

Meanwhile, Paradigm can remain confident that even when those end users inevitably do slip up … SaaS Alerts will be there to save everyone's SaaS.

SaaS Alerts
A Kaseya COMPANY

+1 (910) 887-3352
sales@saasalerts.com
www.saasalerts.com