Terrifying Technology Tales™

VOLUME 3, ISSUE 1.

VISUAL EDGE IT™
SECURE TECHNOLOGY SOLUTIONS

CONTENTS

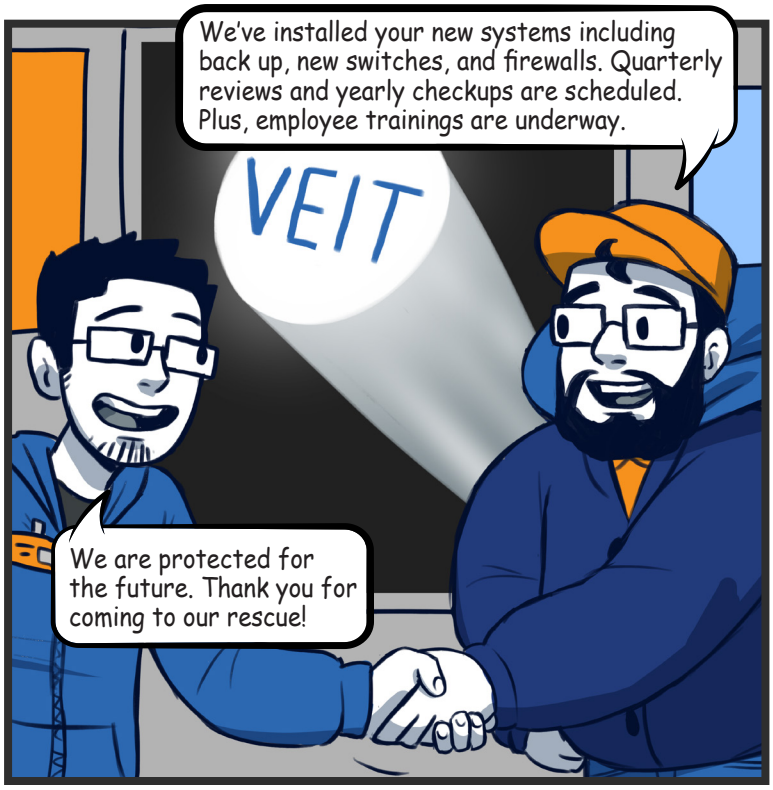
THE RIDDLER STRIKES

What happens when super heroes need a super hero? Send out the VEIT signal, this city is going to need it!

DAWN OF THE DEAD EMAIL

During an early morning email check by the owner of a car dealership, the owner finds his email won't open. After a call to the IT department his worst nightmare is realized.

THE RIDDLER STRIKES



IT SUPER KNOWLEDGE

START WITH THESE STEPS

Verify Emails

Make sure that you verify that the email is valid before you click on links or attachments. Due diligence is key in making sure that situations like this do not happen.

Conduct Employee Cybersecurity Training

Employees are the first line of defense when it comes to network security. Making employees aware of security risks and showing them ways to recognize a possible attack and how to defend them is one of the best methods of stopping an attack before it happens.

Network Assessment

A trusted IT partner can easily conduct a network assessment. This will identify security vulnerabilities and the provider will make recommendations to increase security and reduce cyber threat risks.

Remote Monitoring and Management (RMM)

Remote monitoring and management is the process of supervising and directing client IT systems by means of locally installed agents (software) that can be accessed by the managed service provider. This software alerts the provider on potential performance or security concerns to proactively resolve issues for the client.

To learn more about how to protect your organization, check out these additional resources.

- Network Security Checklist
- Breach Risk Prevention Checklist
- Technology Solutions Checklist

DAWN OF THE DEAD EMAILS

IT SUPER KNOWLEDGE

START WITH THESE STEPS

Recognize you are a target
EVERY organization is a target and no industry is off-limits.

Perform a security risk assessment
Having an assessment will determine what safeguards should be in place that are currently not.

Have a disaster recovery plan
Having a great disaster recovery plan in place can significantly minimize downtime and recovery. It typically consists of a detailed, step-by-step guide that breaks down every aspect of recovery into a clear and concise instruction. If a ransomware situation does happen, you are able to recover quickly along with not having to pay the ransom.

Data Backup and Replication
Backing up your company data is important to keep data secure from being stolen or infected with malware or a virus. Depending on your network environment, the information you want to back up, how often you run backups, and other criteria will determine what type of backup is best for your business.

To learn more about how to protect your organization, check out these additional resources.

- Quick Guide to Ransomware Defense
- Cybersecurity Checklist
- Solutions for Backup & Recovery

Reach out anytime to ask a question or to schedule a no obligation IT security review.

www.visualedgeit.com
(866) 863-2266

VISUAL EDGE IT™

SECURE TECHNOLOGY SOLUTIONS

Written by Sam Lahey. Illustrated by Cassidy Rivers. Layout by Michelle Bates.