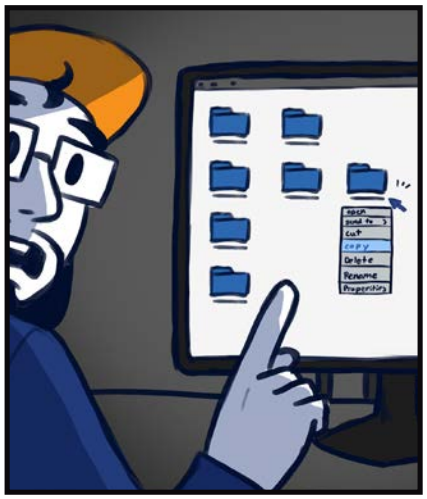
Terrifying Technology Tales™

VOLUME 1, ISSUE 1.

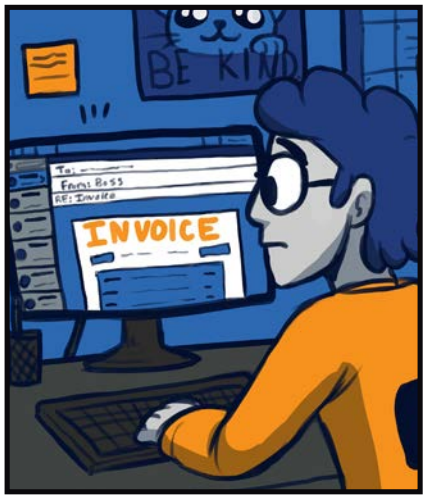
VISUAL EDGE IT™
SECURE TECHNOLOGY SOLUTIONS

CONTENTS



HAUNTED HARDWARE

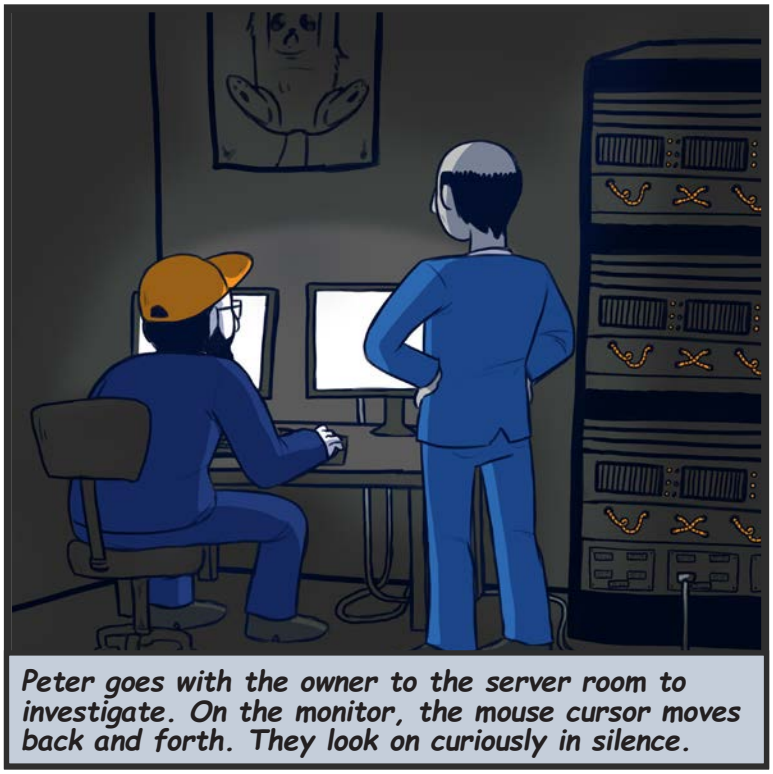
A quiet server room. An unsuspecting business. And a cursor found moving about freely in the dark! Hear the creepy, nail-biting tale of a family- owned business' struggle to get their company data back from Russian criminals.

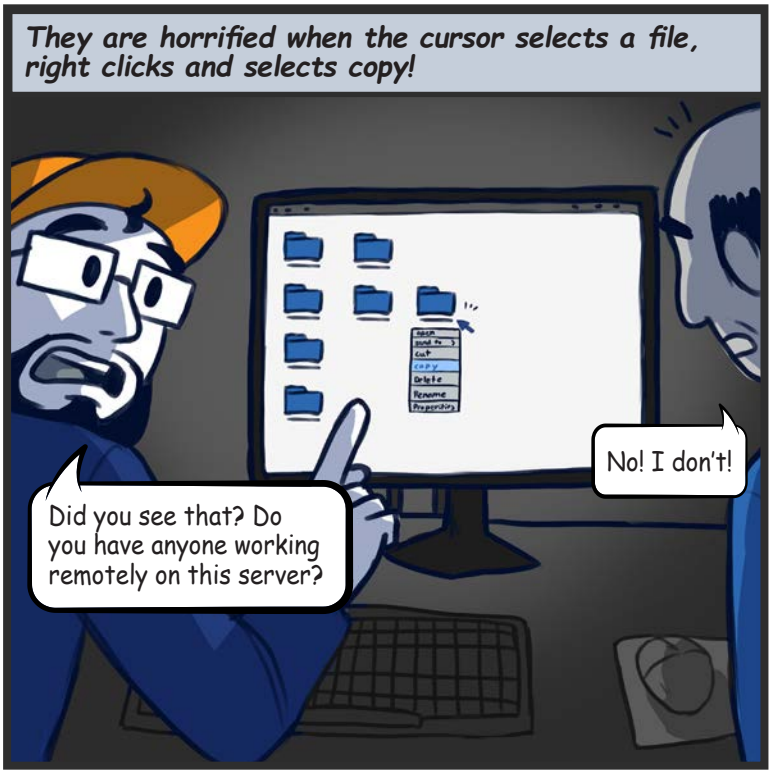


THE TEXAS EMAIL MASSACRE

An unsuspecting employee. A request for verification. And one click that set off a business massacre of epic proportion. Listen-in to find out if there were any survivors of this system slaughter.

HAUNTED HARDWARE





IT SUPER KNOWLEDGE

START WITH THESE STEPS

Firewall

Properly configuring the firewall to not allow remote desktop services be accessed from outside the company and limit access to only those geographic areas they conduct business in.

Security Operations Center

Have an IT partner who provides a Security Operations Center (SOC) that is well integrated with the end user service desk. The SOC watches 24/7 for global cyber security threats and advises the service desk of any issues. The service desk can take proactive actions to alert and protect their customers from cyber criminals.

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.

Advanced Endpoint Protection

Advanced endpoint security uses artificial intelligence to identify and prevent known and unknown threats in real time. Devices can self defend by stopping processes, quarantining those processes and notifying the Security Operations Center to start file rollback.

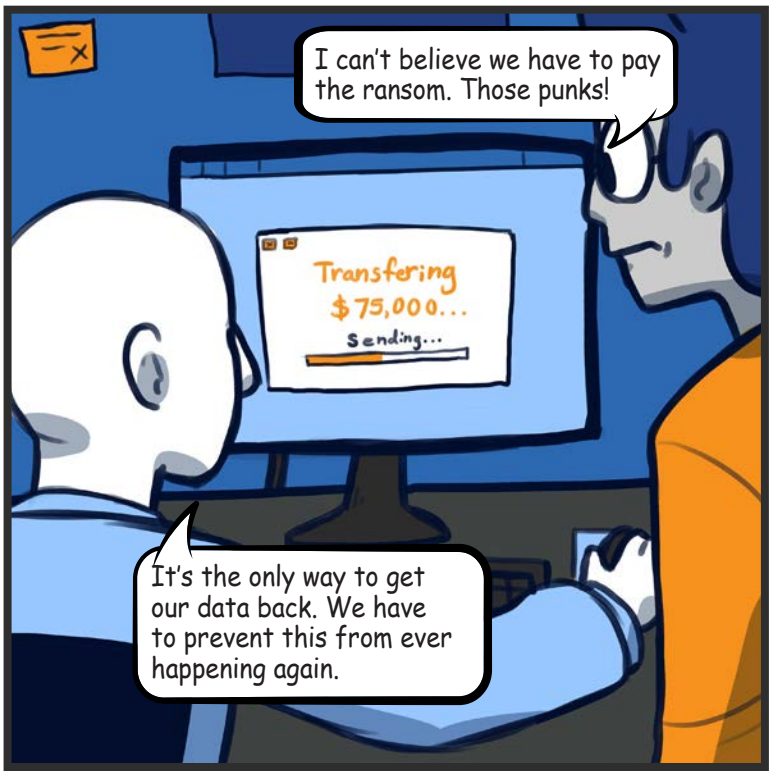
To learn more about how to protect your organization, check out these additional resources.

- Network Security Checklist
- A Quick Guide to Managed IT Services

THE TEXAS EMAIL MASSACRE

An unsuspecting young man is sitting at a computer reading an email from his "boss." He clicks on the email attachment which looks like an invoice.

Elsewhere, a very happy hacker is at his computer when he catches his "phish."



IT SUPER KNOWLEDGE

START WITH THESE STEPS

Employee Education

Keep users apprised of continued threats as technology and attackers are always changing. In addition, ensure there is a quarterly training plan to make sure users know what to do in an emergency.

Backup Disaster Recovery Plan

Having a great disaster recovery plan in place can significantly minimize downtime and recovery. If a ransomware situation does happen, you are able to recover quickly along with not having to pay the ransom.

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.

Company Culture

In order for cyber programs to succeed, there needs to be a top down culture that embraces security as a core corporate value. Choose a partner that can influence senior level perspectives and behaviors to recognize the importance of a strong, proactive cyber program. Align your IT Security with Strategic Business Objectives – with data transformation programs becoming more prevalent across small- and medium-sized businesses, a robust cyber program/partner has never been more important.

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

- Phishing Checklist
- Ransomware 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.