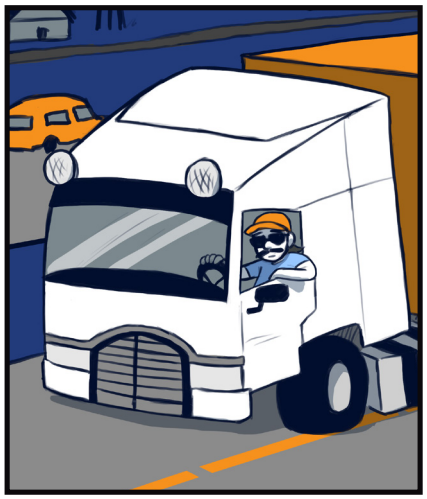
Terrifying Technology Tales™

VOLUME 2, ISSUE 2.

VISUAL EDGE IT™
SECURE TECHNOLOGY SOLUTIONS

CONTENTS



FINAL DESTINATION

A semi-truck driver traveling across country must be aware of potential hazards on his road trip. Careless drivers, poor road conditions and…hackers? Could there be an accident waiting to happen?

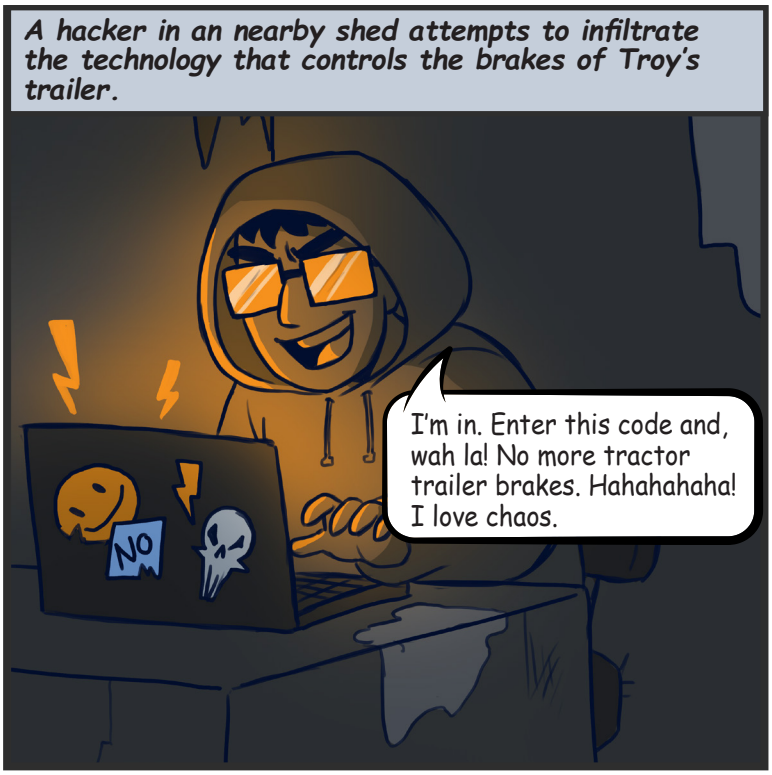
THE PURGE

The owner of a small graphic design firm discovers all her emails have been purged and held for ransom. Having an empty inbox never tasted so bittersweet.

FINAL DESTINATION

Truck driver, Troy, is traveling along highway 52 en route to his shipment customer.

A hacker in an nearby shed attempts to infiltrate the technology that controls the brakes of Troy's trailer.



Unaware that a vehicle hack has been thwarted, Troy cruises along listening to music as he approaches his destination.

IT SUPER KNOWLEDGE

START WITH THESE STEPS

Get an IT Assessment

A network assessment will identify security vulnerabilities. This can easily be conducted by a trusted advisor/IT partner. Your 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. The agent sends information to the network operations center 24/7 so the provider can observe the behavior of the device for performance or diagnostics. This software also alerts the provider on potential performance or security concerns to proactively resolve issues for the client.

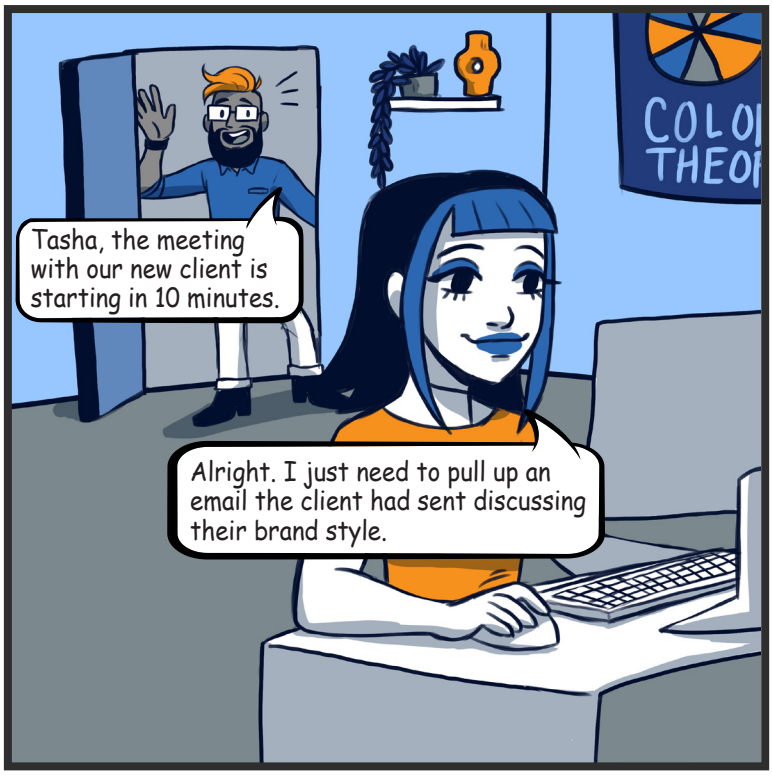
Security Operations Center (SOC)

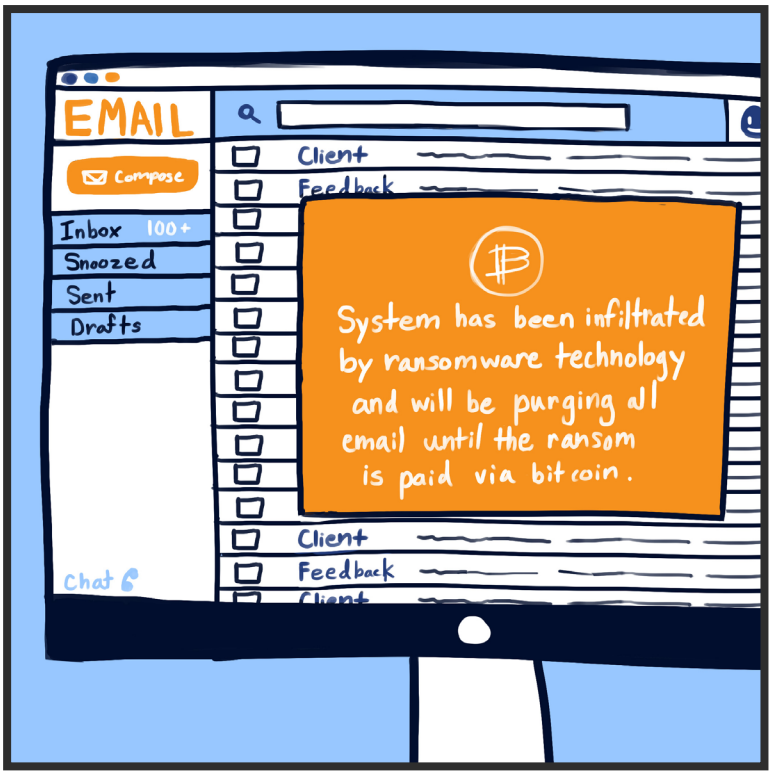
You should choose an IT partner who provides a Security Operations Center that is well integrated with the end user service desk. The SOC watches 24/7 for global cyber security threats and advises the service desk of any issues. The service desk can take proactive actions to alert and protect their customers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

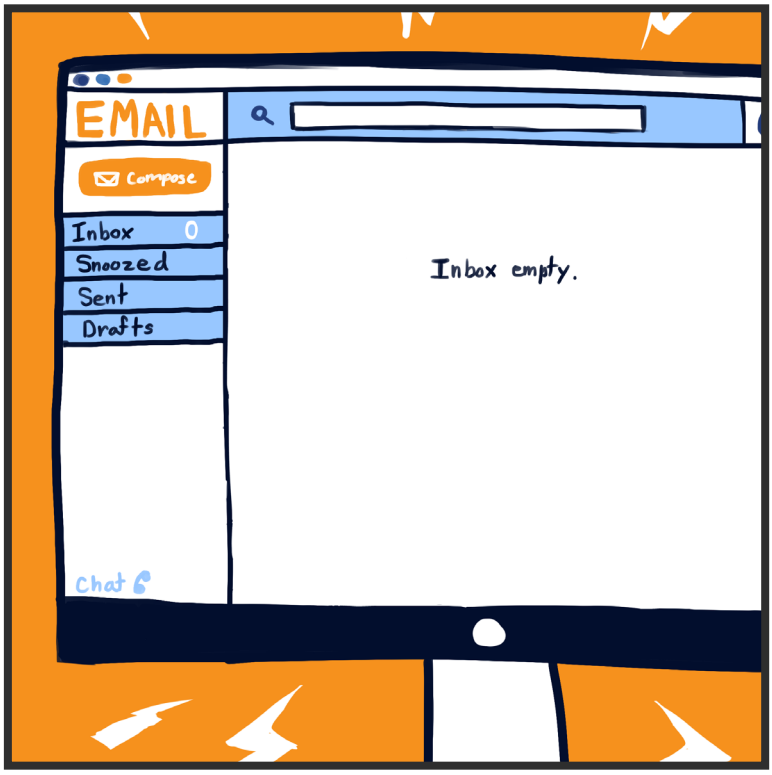
To learn more about how to protect your organization, check out these additional resources.

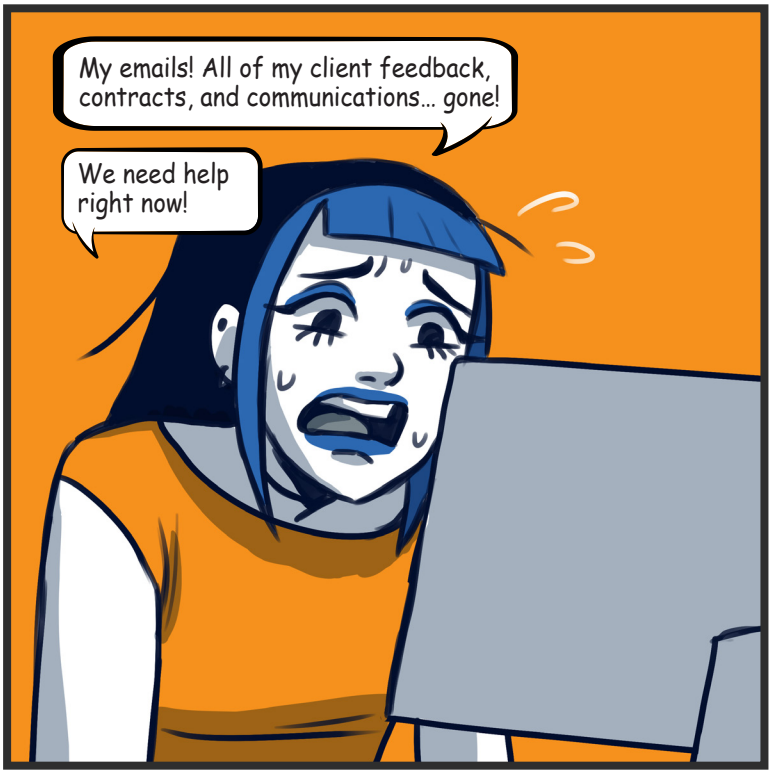
- A Quick Guide to Managed IT Services
- Managed IT Service Provider Criteria Checklist
- Network Security Audit Checklist

THE PURGE









IT SUPER KNOWLEDGE

START WITH THESE STEPS

Shut Down Infected Systems Immediately

To avoid ransomware spreading, disconnect the infected device from any network it is on and turn off any wireless capabilities such as Wi-Fi or Bluetooth. Unplug any storage devices such as USB or external hard drives.

Have a 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.

Security Patches, Updates, and Programs

To stop ransomware from breaking into a network infrastructure, a company needs to be diligent in keeping its implemented software completely updated. Many times, viruses will sneak past security safeguards through gaps in unpatched application security protocols.

Protect Your Network

- Implement a password policy that requires strong passwords that expire every 90-days.
- Implement multi-factor authentication.
- Deploy firewall, VPN and antivirus technologies to ensure your network and endpoints are not vulnerable to attacks. Ongoing network monitoring is also considered essential.

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

- Ransomware Checklist
- Quick Guide to Ransomware Defense
- Cybersecurity Checklist

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

www.visualedgeit.com
(800) 828-4801

VISUAL EDGE IT™

SECURE TECHNOLOGY SOLUTIONS

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