

# TERRIFYING TECHNOLOGY TALES™



VOLUME 3, ISSUE 2.

**VISUAL  
EDGE IT™**  
SECURE TECHNOLOGY SOLUTIONS

# CONTENTS



## OUR WEBSITE'S BEEN HIJACKED!

When a local bookstore finds success online with a website full of children's books, classic novels, and every genre in between, it's the American Dream. But when a hacker redirects the site to one for "Adults Only," the dream becomes a nightmare.



## THE TROJAN HORSE STRIKES AGAIN

How does a logistics company get hacked and lose \$100,000 from its bank account? Easy. The company has never planned and implemented a security strategy for its network. Which makes them a "soft" and unsuspecting target for cyber criminals and a type of Trojan Horse malware.

# OUR WEBSITE'S BEEN HIJACKED!





# IT SUPER KNOWLEDGE

## START WITH THESE STEPS



### Have an MSSP evaluate your current security strategy

As a managed security service provider (MSSP) will tell you, just having security software, firewalls and MFA in place is not a security strategy. Such a strategy should align with your company's vision, and requires an expert to help you contrast it. Sometimes a strategy is built on compliance frameworks like PCI, CMMC or HIPAA. Other times, it can be built around security needs like cyber insurance or industry best practices.

With new vulnerabilities and attack types being released every day, security is a journey, not a destination. Your organization should stem these emerging threats by meeting with your security expert at least monthly, if not more frequently.

### Conduct employee cybersecurity training

Employees are the first line of defense when it comes to website and network security. Making employees aware of security risks and showing them ways to prevent a possible attack is one of the best methods for stopping hackers.

### Don't confuse technology with security

Both fields are related, although security requires a more specific skill set to do it well.

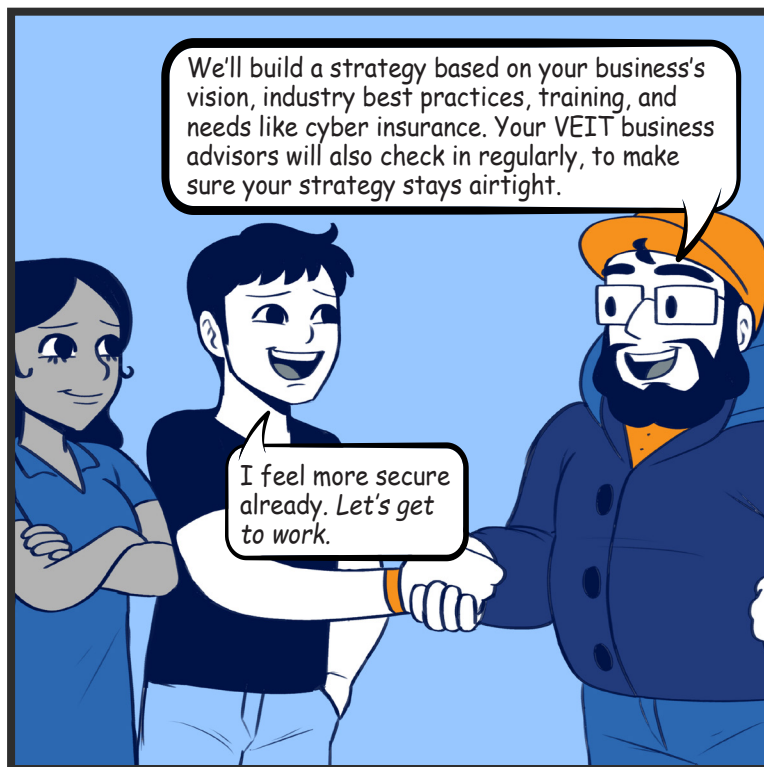
To learn more about how to protect your organization, check out these additional resources.

- [Password Management Best Practices Checklist](#)
- [A Quick Guide to Safe Web Navigation](#)
- [What it Takes to Run a Secure Business](#)



# THE TROJAN HORSE STRIKES AGAIN





# IT SUPER KNOWLEDGE

## START WITH THESE STEPS



### Perform a security risk assessment

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

### Work with an MSSP to develop a thorough security strategy

As a trusted security advisor, a managed security service provider (MSSP) develops a strategy based on your company's own outlook, then helps you contrast it. MSSPs use strategy cornerstones such as industry best practices, cyber insurance, and compliance requirements for HIPAA, PCI, CMMC and others. An MSSP also works with you throughout your security journey to guard against new cyberattack types and vulnerabilities.

### Test incident response plans and business continuity plans

Without testing to ensure these plans are applicable and work effectively, your organization will not be prepared when a cybercrime event occurs.

### Other useful security strategy practices

- Require two people to sign off on every business transaction.
- Make sure employees use strong passwords that are difficult to crack, and enforce password policies that require regular password changes.
- Employ multi-factor authentication practices to access networks and systems; MFA requires users to provide two or more forms of ID, such as a password and a token or a biometric identifier.

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

- [Keep Network Doors Closed to Prevent a Security Breach](#)
- [7 Reasons Why Security in Networking is Important for Your Business](#)
- [Network Security Audit Checklist](#)

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

**[www.visualedgeit.com](http://www.visualedgeit.com)**  
**(866) 863-2266**



Written by Tom Bailey. Illustrated by Cassidy Rivers. Layout by Michelle Bates.

© 2023 Visual Edge IT. All Rights Reserved.