MAKE IT EASY

NETWORKS, PRINTERS, PHONES AND SECURITY

1997-2022 25 YEARS GREAT BUSINESS RESULTS.

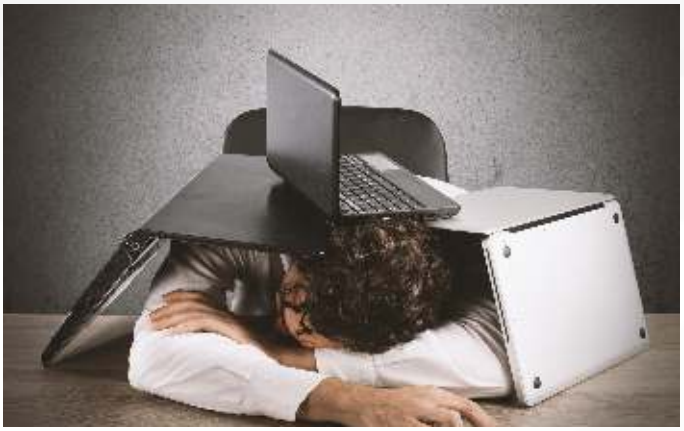
CYBERSECURITY FATIGUE

DAVID WOLF

VICE PRESIDENT OF JUST SOLUTIONS INC.

Are you and your company suffering from cybersecurity fatigue? After a while, we get numb to all the "bad" news in the world. Covid still exists but people are "over it". The public is tired of hearing about Covid. Do you remember the daily stats on the news every night? The constant reminders to wear a mask, social distance, wash your hands, get tested and of course, get a booster shot? It's exhausting.

Unfortunately, cybersecurity fatigue is real. Companies and users are tired of hearing about passwords, security awareness training, and breaches. Oh well, Uber was breached again. People don't care until it finally hits them at home or at work.

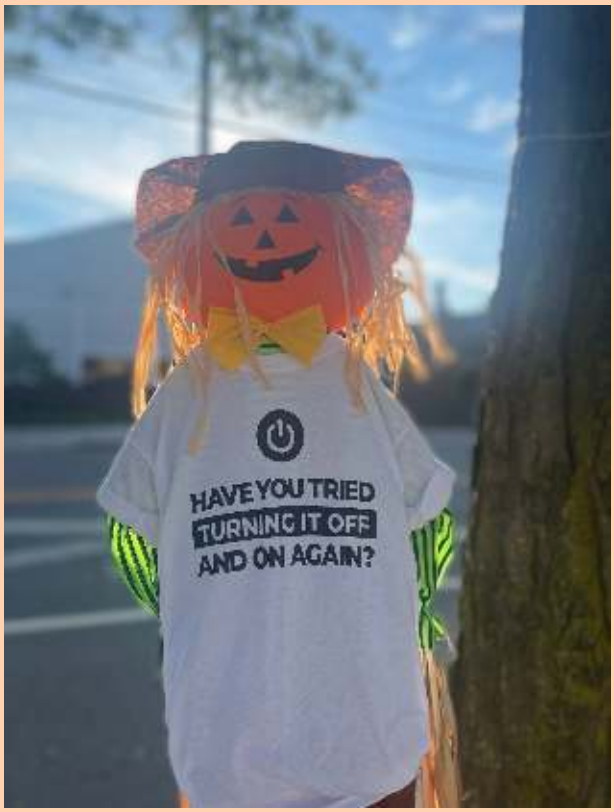


We at Just Solutions have seen a large uptick in business email compromises (BEC). Small businesses and individuals are having their email breached and intercepted. Payment details for bills, purchases, house closings are all getting manipulated and their bank routing information altered by "man in the middle" email scams. The amounts have ranged from $30,000 to $150,000 stolen via BEC. There was no network hack. Users are being tricked into sending the money to the wrong accounts. Customer/vendor relations are being damaged as each side blames the other for the fake emails.

IT'S CYBERSECURITY AWARENESS MONTH

The theme for the month is "it's easy to stay safe online" and Just Solutions is proud to be a champion and support this online safety and education initiative this October.

Happy Halloween



FBI research shows that BEC is currently the costliest digital crime, far surpassing ransomware, to account for US $49.2 million in victim losses in 2021. BEC is also known as email account compromise (EAC) or 'man-in-the-email' scamming.

I have been "preaching" about cybersecurity for years now. I write blog articles, send out email reminders, tell my clients repeatedly to stay vigilant – and I still get clients that are "in shock" when it happens to them. The common response I hear from them: **"I thought we were protected from this."** It is difficult to explain that they have been duped, tricked, or scammed. It usually starts with a phishing email. They respond to an email or a website popup and voluntarily gave their credentials to the cyber thief.

#BECYBERSMART

The Real Treat Is Staying Cybersecure All Year Long.

MEEET THE TEAM

With over 20 years of experience and his CISSP under his belt, a CCSA (Sonicwall Network Security Basic Administration) certification, a CompTIA Security+ Certification, and experience as a Senior Project Manager and Network Administrator at Soyata Computers, Brian knows a thing or two when it comes to IT.

His favorite part about showing up every day is "empowering clients with security and technology solutions to help them gain a competitive edge in their market." When he's not busy securing our clients, he enjoys camping with his family, and cooking & smoking BBQ.

BRIAN HILGERT
CHIEF SECURITY OFFICER
RED TEAM

Every type of “attack method” from cyber criminals has an appropriate countermeasure. Yes, technical stuff that I don’t expect you to know, but your IT department better have in place. For BEC, the following items need to be in place:

For BEC, the following items need to be in place:

- DKIM, DMARC, and SPF configuration of your email and domains.
- Anti-spoofing/anti-spam scanning of emails with quarantine. Yes, "sandboxing" the attachments and testing them to make sure they are clean.
- Checking for misspelled domains. We have found clients tricked by email domains with one extra character in the name or the wrong domain suffix.
- Constant user awareness training is a must.
- The biggest requirement of them all is multi-factor authentication (MFA). I have been repeating this over and over. Many clients don't want the "hassle" of MFA as an extra step to log in. At this point, I say "too bad" – turn on MFA now before you are breached. I hate to be the "I told you so" kind of guy, but MFA is a must. We still don't have all our clients compliant. Thank goodness insurance companies are now requiring it for businesses to obtain cyber insurance.

I know those bullets contain a lot of “technical stuff" – I am happy to explain and review it with you and your team. I know we are all tired about hearing about breaches and cybersecurity, but it is a billion-dollar problem that is not going away. So, get smart and get prepared now. Every day, every hour there is a new business who has fallen victim.

WHAT OUR CLIENTS ARE SAYING

David Hornbek, Sr.
OPERATIONS DIRECTOR

Dedicated To Your Success.

"I just wanted to drop you a note to say how much we appreciate your team!

Recently, Justin and Rich helped us with an issue and got things working again for us in record time. We have worked with others on your team and can say the same as well.

We appreciate the courtesy, professionalism, and speedy solutions that we encounter every time we contact your company."