THE GREAT EMAIL HIJACK

How criminals break into your email to plunder your business bank accounts as well as you company secrets. Yes, each and every business is currently under attack, every day...

and this is what to do about it

By Alan Helbush

THE GREAT EMAIL HIJACK

How criminals break into your email to plunder your business bank account. Unfortunately, every business is under attack, every minute of every day...

and this is what to do about it

By Alan Helbush
Where To Start, Inc.

THE DISCOVERY

David sat back in his chair, the blood draining out of his face as the implications of what he had just discovered began to sink in.

Just over $12,000 has been stolen from his business bank account. The money had been intended for a critical supplier that still hadn't been paid, and it is a significant hit to his cash flow of more than $24,000.

How?
How??
How did this happen???

It wouldn't kill the business. But it would make things very tough for a few months.

What would he tell the staff?
What would he tell his wife??
Would his clients find out???

Today had started with the hope being a lot more promising...

But, after 10 wonderful and relaxing days in Orlando with his wife and family, David had got into the office at 7am, keen to catch up on the hundreds of emails that inevitably waited for him.

As the owner and CEO of a fast-growing business, it was rare for him to be away from his email for more than a few hours. But he'd promised the family this would be a proper vacation.

Which meant no phone calls, no emails. Just family time as it should be.

He'd checked in with his operations manager from the airport two days ago and knew there were no significant issues he needed to deal with before Monday. So he had felt very relaxed and ready to get back to work this morning.

It only took 23 minutes for that to change.

"Please can you tell me when this month's invoice will be paid? It's now overdue," the email from the key supplier had read.

David was puzzled. He'd left specific instructions for this supplier to be paid on time and looked after to ensure nothing goes wrong. And when he logged onto a business banking account, he could see the payment had left the bank account.

Clearly, this must be a misunderstanding. So he emailed his supplier's CEO back to tell her when payment had been made, and everything was OK.

She'd apparently made an early start on Monday as well, as she called David within 5 minutes of him sending his email reply. Unfortunately, after the usual pleasantries, she'd said they hadn't received the payment as he thought.

David promised to look into it and get back to her. And that was when the sick feeling started in the pit of his stomach.

He logged back onto business banking and looked more closely at the payment.

The right amount had been paid on the correct date. Using the correct payment instructions.

Thinking this is weird.

He arched his fingers and sat back in his chair as he thought through the problem.

The payment had been made 5 days ago and hadn't bounced back.

That was when he thought to check the payment details against the invoice.

Oh. Wow.

The bank routing number and account number that the cash had gone to were completely different from the ones on the invoice.

Now the sick feeling was getting stronger as he pressed a button on his phone and called his operations manager.

It was a phone call he would never forget (although he wished he could). *"Yep, I got it all sorted out, boss," his ops manager said. "I paid it the day after they emailed it."*

"But they haven't had the payment," David replied.

"But, maybe they're checking their old bank account still. And I paid it to the new one."

Wait. What was that?

"What new bank account?" David asked, now he is deeply alarmed.

"Oh, they've moved banks," his second in command answered. *"Just after they sent the invoice, they sent another email with the new bank details. I amended the bank mandate to make life easy for you..."*

SADLY, THIS IS NO LONGER AN UNUSUAL SITUATION

Hello, my name's Alan Helbush. I'm a local small business data security and IT expert and the owner of Where To Start, Inc.

Yes, it saddens me to tell you that – while this may be a fictitious story, the situation David has found himself in is no longer rare, but commonplace.

In fact, at least once a month, our phone rings, and we find ourselves talking to a business that has found itself compromised in some way (these are not existing clients we are protecting, I hasten to add).

The outcome is almost always the same – money has gone from the business bank account. Stolen and, in most cases, not recovered.

9 times out of 10, the entry point is the same too. An email account somewhere in the business has been compromised somehow, used to gather information, and then manipulate the system.

When you think about it, the very nature of email makes it the the weakest link to any security setup.

For many of us, email is both an incredible tool, and it can be our most hated nemesis at the same time!

You have lots of staff accepting hundreds of emails every day. And even the best email filters in the world can't stop clever criminals. Because they're constantly inventing new ways to get in and very profitable for them.

All they need is one member of your staff to click one lousy link, Game Over. That can give them enough access to start observing what the business is doing. From there, they can spot ways to access business funds, identify other business assets (targets) and companies you rely on outside of your business.

If a criminal can get control of your email, they can determine patterns and usually access multiple other systems and applications at the same time to manipulate the conversation.

Why? Because when you forget your password on most systems, you enter your email address, and it emails you a link to click. That huge convenience comes at a terrifying cost.

Shortly, I'll tell you about the most common email frauds we come across. But for now, let's return to David's bad day and see how his business has been impacted.

NOW THE HASSLE

David slammed the phone down in anger and swore. What was the point of having a relationship manager at the bank, if he couldn't help him in an emergency?

It was only lunchtime, and so far, his morning had been terrible. First, he'd looked at the email his operations manager had received from the supplier, with the new bank details.

It did seem to come from them. Yet something about it didn't quite feel right. David couldn't put his finger on it.

Clearly in a rush last week, his ops manager had accepted the new account details at face value and hadn't given a second thought about it.

Losing his temper, David had shouted at his ops manager and called him stupid. In front of the other staff. That was a big mistake, and he needs to apologize for his action by the end of the day.

Now his ops manager was fuming at his desk, going through all mandates from the bank and phoning up suppliers to check the details were correct. While they were pretty certain no one had got into the bank account itself, David didn't want to take on any more risks from now on.

The rest of the staff was working a lot more quietly than usual. Whispers were going around of the business about having all of its cash stolen and them not getting paid. David knew he'd need to talk to them all this afternoon and reassure them they would get through this.

He'd phoned his crucial supplier, and thankfully she was happy to wait till the end of the week for payment. She was clear they hadn't sent the dodgy email.

David wasn't looking forward to telling his wife he needed to take $20,000 out of their personal savings to meet that payment, and then paychecks on Friday. They'd both believed the days of emergency loans into the business were long gone.

The phone call with the bank hadn't gone so well. After holding for 20 minutes while the relationship manager spoke to his immediate supervisor, he said there was nothing the bank could do to help.

They would attempt to get the money back from the bank the payment had been sent to. But, in his experience, that money would already have been removed, and the bank account abandoned. So it was unlikely anyone would be able to follow the payment chain to the end.

While holding, David did something we all do; he Googled for advice, and to be honest, that didn't make him feel any better. Because his business had authorized the payment, the bank didn't have any legal obligation to refund the business.

David picked up the phone again and called his IT support company. If the bank couldn't help, their IT support company would shed some light on the situation. ***NOTE:*** *This call should have been one of the first calls he made this morning.*

Well, that call didn't go well either.

It took the technician on the helpdesk just a few minutes to spot how the fraud had happened.

"If you compare the two emails – the real email from your supplier, and then the fraudulent email pretending to be from your supplier – you can see the domain name is slightly different," he'd said.

"The hackers have been monitoring your email for a while and spotted that you regularly pay a considerable amount to this supplier.

"So they registered a new domain name that is similar to your supplier's domain but has an extra character in it – look, there's an extra 'e.' Can you see it?"

David had peered at the email address. Oh. SH!T. The technician was right.

"So all the hacker had to do was wait for you to receive the invoice and then immediately send the fraud email pretending to have sent you the wrong bank details. Very simple, very clever, and very effective."

"I feel so stupid," David said.

"Don't," the technician replied. *"Lots of people fall for this, in the rush of getting everything done every day because we are not being taught what to look for.*

"Now, what we really need to figure out is how they got into your email system in the first place, kick them out, and stop anyone from getting in again."

David felt his face start to turn red as something occurred to him. *"Isn't this something you guys should have stopped anyway? You are my IT support company, after all."*

There was a pause on the other end. Then the technician replied. *"Well, we're not really cyber security experts. We did offer you some extra protection last year, but you declined it."*

David thought hard... and then remembered. First, he had dismissed the idea of extra protection. Then, he recalled the exact words he had used.

"We don't need that... it'll never happen to us because we are too small and don't have anything they want."

COMMON EMAIL SCAMS AND HACKS

For far too many businesses, email security isn't an issue... until it suddenly is.

Not enough businesses have put a proactive, preventative security strategy in place until its to late and they've been hacked. But, unfortunately, that's like waiting until you've been burgled to put locks on the door.

There are lots of different types of email hacks. But, these are the most common ones we have either seen ourselves or heard about from our network of international IT security experts.

Email forwarders: This is where criminals gain access to your email just once and put in place an email forwarder. Then, without your knowledge, all incoming email is forwarded to them as we as to you. They might not be able to see every reply you send, but it's usually relatively easy for them to spot patterns, such as invoices being sent to you regularly. An email forwarder is often the starting point for hackers. From there, they can play a long game, gathering information and building up a profile of their target until an opportunity presents itself to steal money or other types of business data.

Spoofed emails: Just as David discovered, one scam is to buy a domain name that's very similar to the actual domain used by a supplier. So your supplier might use xyzcompany.com. And the hacker acquires the xyzcommpany.com domain. An extra character can often go unnoticed. Another trick is to buy a mail domain with a different extension, such as a .net rather than a .com.

Follow-up emails: Exactly as David's ops manager was deceived. Yes, the follow-up email is a clever trick. But, the criminals have to get the timing right for this. If they can send a follow-up email immediately after an actual email, most people assume it's real and trust the second email as creditable.

Compromising the email supplier: It doesn't have to be your the business that gets hacked to lose money. If they can compromise your email supplier's and intercept the outgoing invoices, they can get a range of customers to pay money to the wrong bank account. Flip that around, and imagine if a criminal adjusted all of your invoices. So your customers were making payments, but not to your bank account.

Edited PDF's: Many people think a PDF within an email is a safe document. Yes, PDFs can be easily modified for malicious deeds. For example, we've heard of criminals intercepting invoice PDFs, editing them to change the bank routing details, and then sending them on to customers. This is a very clever hack because the person paying the invoice will typically have zero suspicion.

Using key-loggers to directly access bank accounts: The use of specific malware that sends back information on every button you press directly to the criminals. They can use this to see you have visited a bank's website, and over a period of time, put together much of the information you use to log in.

Social engineering: Once the criminal is inside your email, they will gather information and look for opportunities. A golden chance for them is when the boss is on vacation. Because that's a break in typical patterns of behavior, then they leverage it. We have heard of one company where the boss's email had been compromised, with an email forwarder set up.

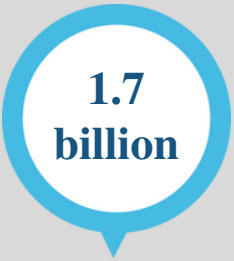
The criminals couldn't send an email from the account. But instead, they set up a Gmail account in the boss's name and emailed someone senior in the company. "My work email's not working, so I'm using my personal email," the message read. "Great beach weather here. I forgot to pay an invoice before I left the office – can you pay this ASAP, please". Inevitably, the staff didn't think twice. Yet in another example, the criminals sent a Gmail pretending to be the boss and said they'd been locked out of their Office 365 account. They asked the office administrator to reset their password. And gained themselves full access to the boss's email while he was sat on the beach, unaware he'd been hacked.

Staying on that theme – if there were one thing we would try to enforce within every business we protect, it would be this: **Establish a Protocol and Never let the boss break the protocol!**

Businesses put in place systems designed to protect them. Then the boss will send an email asking for an urgent payment to be made. And usually, the staff will comply! (Stop doing this).

This sets up circumstances for easy fraud. Any criminal sitting monitoring email traffic will see this happening and know it can be leveraged. **It WILL be used against you.**

Before we re-join David's story, **here are just three email hacking stats we have gathered over the last few months:**



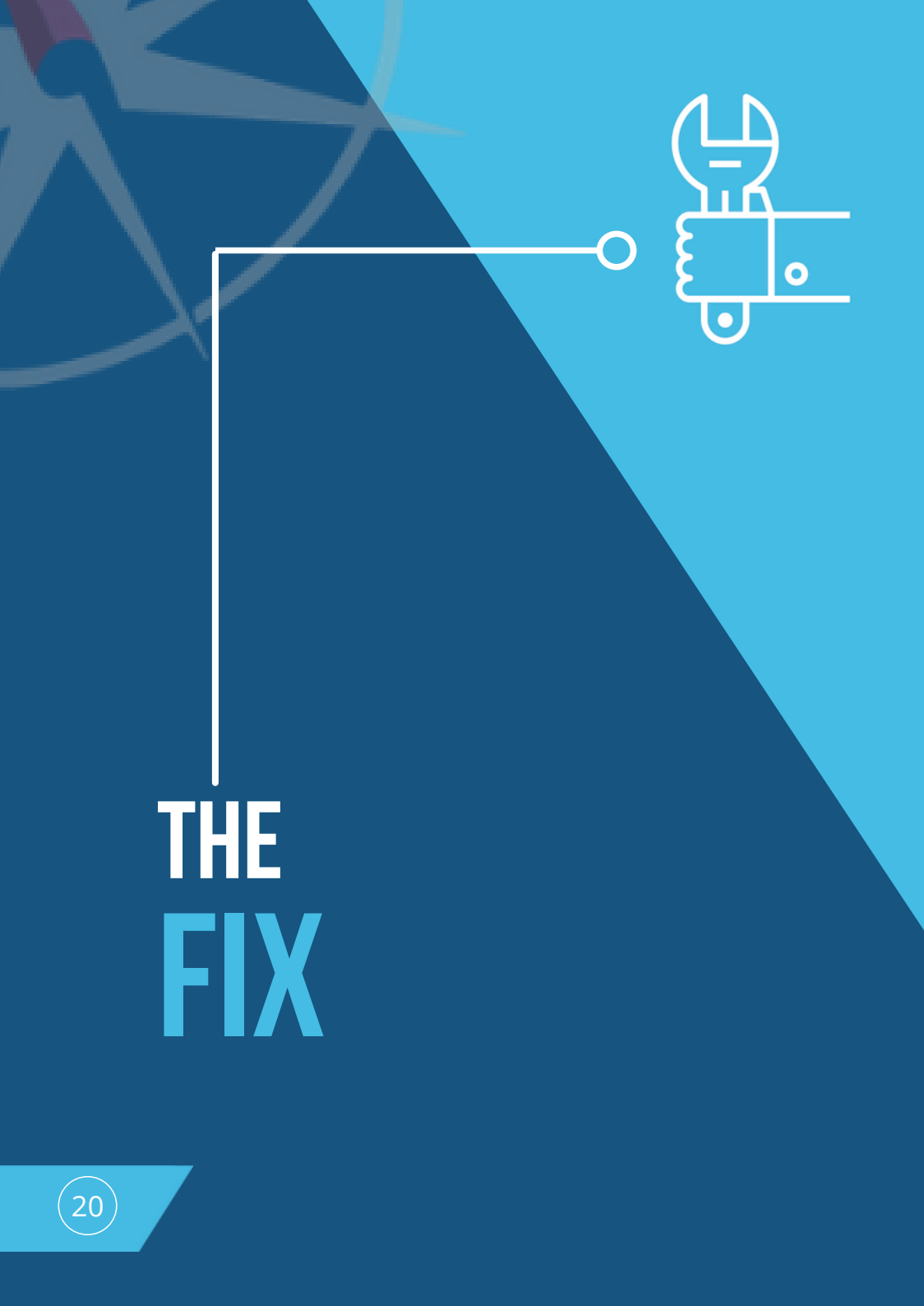
There are 1.7 billion pieces of malware out there, all trying to infect your inbox.

Criminals make a bunch of money from cybercrime, with a reported return on investment of 1,425%!

60% of all companies have experienced a data breach in the past 2 years... many of which are the result of poor email security

There are many scary stats out there – just Google "email security stats" to see for yourself, pick a few for your staff meeting.

Now let's re-join David as he gets the experts to fix his email security breach.



THE FIX

"It's sometimes impossible to pinpoint the exact entry point into your email system," a new voice on the phone explained to David.

"So our focus after a breach is a broad series of 'best practice' security measures to ensure it won't happen again. We have a full checklist of things we will do to kick your criminals out and prevent them from getting in again."

He continued: *"There are no 100% guarantees with cyber security, as it's such a fast and moving world. But what we're going to do for you will make your business dramatically harder to break into in the future.*

"Criminals like low-hanging fruit. Your business's fruit will be much higher up the tree."

David felt his body starting to relax for the first time in 24 hours. However, he had a terrible night's sleep, getting home late and waking covered in sweat at 4am.

Since he'd discovered the theft yesterday morning, it had consumed every moment of his day and every last bit of energy he had.

He had got a lot sorted out – including placating the staff, and apologizing to his ops manager and the team.

He'd also decided to hire a new IT support company. They were a lot more focused on cyber security than his previous company.

And he believed them when they said cybercrime was the number one threat to businesses like his.

Pity, the hundreds of vacation emails, we're still waiting... and now, his staff were going to have to suffer a load of disruption, as the business's security was locked down.

The new IT support company immediately logged everyone out of their business email accounts and forced everyone to change their password. Of course, there were a few grumbles, but the team could see why it needed to happen and understood the sense of urgency.

They also had multi-factor authentication set up. *"It's just like when you login to your bank account or use the ATM,"* David explained to his staff.

"You use an app on your phone to confirm the login and prove it is you. The new IT company tells me it's a minor disruption but immediately stops us from being an easy hack in the future".

The firm's technicians investigated the email trail that had led to the hack and quickly discovered an unauthorized email forwarder.

Cleverly, the hackers had set it so it couldn't be discovered in normal Outlook email – only in Outlook Web Access, where you get your emails through a browser. That explained why David's old IT support company had never found it.

They deleted the email forwarder, reported the email address, and then set up a scanner so they'd be notified if an email forwarder was ever set up again. They also set up and turned on a complete audit trail within Office 365 to help diagnose any future hacking attempts.

Additionally, they reported the dodgy domain name where the hackers were pretending to be David's supplier.

This flurry of activity seemed enough to David. But the reassuring voice on the phone also said there were other areas they really should address.

"The goal is to put together a layered security solution, to offer you the right balance of security and risk," he explained.

"We want you and your staff never to have to go through this again. But at the same time, we don't want to create too much adverse disruption to the way you work every day."

David listened intently. "*Studies have shown that too much security can have an adverse effect on staff attitudes towards it,"* the technician continued.

"They will soon forget the pain of this hack. But, if they see the ongoing extra security as an annoyance that's holding them back, they will not take it seriously. And that could leave you even more exposed than you were before.

"So together we're going to find the right balance of security, risk and education required for the business."

David scribbled notes on his pad, as the technician laid out the many different options available to him. Even at this early stage, he could see some would work well with his staff, and others were impractical.

It made him feel more relaxed that he had an expert on his side, helping him get this sorted out properly going forward.

YOUR 9 LAYERS OF SECURITY

If every business used every possible layer of email security, they'd reduce their chances of being hacked down to just 1% or 2%.

But they'd also struggle just to do business every day.

Because there are plenty of tools available to protect companies of every size. The trick is – as the technician explained to David – is putting together the right balance to suit your business and risk. So you're protected, but your hands are not tied.

Here are the 9 layers of email security we normally consider for every client we're protecting. This is not intended to be an exhaustive list. It's a start point of 'best practices' that the average business should pick and choose from, using expert help for guidance.

1 - Multi-factor authentication: The simplest but also the most effective way to prevent unauthorized logins. Every time you log in to your email (or any other system), you have to confirm it's you on a separate device. This is typically done via your mobile phone, either by receiving a code or using an app to generate a code. To counteract a new crime called 'simjacking,' where criminals clone your cell number to their device and intercept your multi-factor authentication alerts, there is also the option of using special devices plugged into your laptop.

2 - Monitoring for unauthorized email forwarders: As David discovered, these criminals play a clever long game just by accessing your email once. An unauthorized forwarder allowed them to monitor communications. It doesn't even need to be the email of a senior member of the team. It's surprising (and terrifying) how much we give away, bit by bit, in our daily emails.

3 - Proper email backup: Unless you have bought specific

email backup, your emails are not being backed up and so are not protected daily. Unfortunately, not many people realize this. Having a proper backup is critical, as it gives your IT support company so many more options if you are attacked. They can completely reboot your email account, safe in knowing you won't lose a single email.

4 - Artificial Intelligence (AI) screening of emails: You have this contact named John. And then, one day, he signs off an email with his full name, Jonathan. You might not think twice about it. But an AI system would pick up on this sudden behavior change and investigate the email further. These systems can be very clever at spotting potentially bogus emails from the tiniest of symptoms.

5 - Improved security on the endpoints: OK, heads up on this one. I just used some internal IT gobbledygook. Sorry about that. What it means is that each computer you use to access email is locked down and protected. There are many different ways to do this. From enhanced security on each device to prevent it from being used for risky activities. Encryption of the data on the device, meaning it's to anyone

that steals it. And even as far as banning USB devices (you can plug them in, but they won't work... translated, they can't do any damage).

6 - Office 365 Advanced Threat Protection: At the risk of dropping more gobbledygook again (it's OK, I won't) – you will want this. It's robust Microsoft protection working for you behind the scenes. But your IT support company will know the correct method to implement it for your specific setup.

7 - Awareness training: The weakest link in any email security setup is... well, it's the human. Because harmful emails will still get past all of the defenses I've already listed, the last line of defense (and frankly, the best) is the human looking at an email with suspicion. However, there are some fantastic awareness training courses available. They're delivered online, so your team doesn't have to go anywhere. They're not dull or techy. They're designed to be fun, and above all, to make your staff pause when they're sent that bogus link to click. That pause can save you thousands of dollars and days of hassle.

8 - Cyber Insurance: The jury is still out on the value of cyber insurance as it stands today. It could very possibly become a 'must have' insurance in the years ahead. It could be worth you taking out a policy today if only to follow the basic standards laid out by the insurance companies. Honestly, it's their job to reduce their chance of having to pay out, right? That means they're highly likely to know what the 'best practice' currently is. So follow their advice as part of your overall email security protection.

9 - Set up business processes and make them the culture: I said this in a previous chapter – don't let the boss change the process on the fly! If you have an internal process for approving payments, it needs to be followed every time... ESPECIALLY when it's inconvenient for the boss. Because it's when the boss cuts corners that the chance of fraud jumps up dramatically, remember the weakest link is the human behind the keyboard. And when it's the boss and everyone wants to please them, but as we know, that opens the window for fraud. And encourages everyone to break the rules now and again. Great leaders realize they need to act the way they want their staff to work... even if it's an inconvenience.

THE FUTURE

David laughed at the joke as he took a bite of his food. He always enjoyed the company of this particular group of friends, as they were business owners too, just like him.

Their spouses and children had grouped together and gone off to do their own thing. So the conversation soon turned to business.

After the usual bravado of everyone claiming the business was great, they started swapping horror stories.

They talked about how members of their staff really should be fired.

All had some major customer service failures.

The idiot client they could all relate to.

And David, he couldn't help but chip in with his story from a few weeks before. He told it in great detail with all the embellishments, of course.

The discovery. The hassle. The fix. And how just a few weeks later, his cash flow was starting to recover, and how he knew the business would be fine.

He had everyone's attention, and they all jumped in with loads of questions for him.

As he listened to them discussing the situation, he remembered something his new IT technician

had told him on the phone.

"Far too many businesses, email security isn't an issue... until it suddenly is."

David knew that had been the case with his business. Now it was protected and kept up-to-date.

He'd read stuff over the years about cyber security but had assumed hackers wouldn't be interested in a business like his.

Now, he knew the assumption was completely wrong. Business owners and managers were busy all the time, that they had to filter out a lot of the noise.

He realized cyber security was suddenly much higher up the agenda for this group of friends because someone they knew had been attacked and compromised.

In the same way that people buy home alarms systems when a friend has been burglarized. And more insurance when someone they know well has a severe illness.

If that was the one good thing to come out of this expensive, difficult lesson, then David could live with that.

He swigged his beer and smiled.

WHO DO YOU KNOW, WHO'LL BE COMPROMISED NEXT?

As I said earlier on, while this is a fictitious story, but the situation David found himself in is no longer rare, but commonplace.

I'm not scaremongering when I say someone you know will be compromised at some point in the next 12 to 18 months.

You might not know about it because business owners and managers don't like to run around telling everyone and especially their clients, they've been hacked. So, understandably, they are reluctant for clients and peers to find out even though they still believe they did nothing wrong in most cases!

Which is a pity. I wish more business owners would tell their friends when it happens. Not because IT security and support businesses like mine enjoy cleaning up the mess afterward. Far from it, it is because it will increase awareness...

We prefer doing preventative work to stop it from happening in the first place.

It's easier for you to make decisions about the appropriate blend of security for your business when you're doing it by choice rather than in a hurry as a matter of necessity.

It's also a lot less expensive. And there's considerably less hassle for you and your team.

If your business isn't yet fully protected with the correct layers for your specific situation, my team and I would love to help you. Finally, more and more owners and managers are waking up to the risks and implementing appropriate preventative measures.

You may get in touch with us at:

- www.WTSci.com
- hello@WTSci.com
- (844) 727-6448

Schedule a Video Chat with us

Meantime, if you are happy with your blended email security, please feel free to pass this book onto a friend who maybe isn't quite as ahead of the curve as you.

Thank you for your time, and I hope you found it worthwhile reading.

IS YOUR EMAIL BEING HACKED YOUR WORST NIGHTMARE?

Well, Maybe it should be. Every day, every single business in the world is being targeted by criminals. And it most likely starts with an email.

These aren't the young script kiddies of the 80s and 90s who were breaking into systems just for the challenge of it.

Today it's a highly organized and lucrative crime. These criminals are using intelligent, automated tools constantly testing every business's armor, looking for just one tiny crack in their defenses that will let them get in and gain a foothold.

And their favorite access point is your email. Because with a little patience, and some innovative thinking on their part, your email can provide direct access to the contents of your business's bank account.

This book is an essential read for every business owner and manager.

It uses the fictitious story of a business owner to explain complicated cyber security concepts so that anyone can understand them.

We are also providing you with a checklist of 9 powerful defense weapons so you can create a blended security structure for your business.

The author, Alan Helbush, is an acknowledged data security expert. He owns Where To Start, Inc., where he has been securing organizations, small and large, for over 20 years.