YEO & YEO
COMPUTER CONSULTING

EMAIL HIJACK

How hackers break into your email to plunder your business bank account.

989.797.4075 · 800.607.1446
yeoandyeo-consulting.com

EMAIL HIJACK

STOP HACKERS FROM STEALING YOUR DATA

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 stolen from his business bank account.

And, because that money had been for a key supplier that still hadn't been paid, a total hit to his cash flow of more than $24,000.

How? How? How???

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?

Today had started a lot more promising...

After 10 days in Orlando with his wife and family, David had got into the office at 7 a.m., 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 holiday, which meant no phone calls, no emails.

He'd checked in with his operations manager from the airport two days ago and knew there were no major issues he needed to deal with.

So he felt very relaxed and keen 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 supplier read.

David was puzzled. He'd left specific instructions for this supplier to be paid on time and well looked after.

And when he logged onto business banking, he could see the payment had left the bank account.

Clearly a misunderstanding. He emailed his supplier's CEO to tell her when payment had been made.

She'd made an early start to Monday as well, as she called David five minutes later. After the usual pleasantries, she'd said they hadn't received the payment.

David promised to look into it and rang off. 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, paid on the right date, using the correct payment mandate. Weird.

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

The payment had been made five 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 those on the invoice.

The sick feeling was getting stronger as he pressed a button on his cell and called his operations manager.

It was a phone call he would never forget.

"Yep, it's all sorted out, boss," his ops manager said. "I paid it the day after they emailed it through."

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

"Maybe they're checking their old bank account still. I paid it to the new one."

Wait. What was that?

"What new bank account?" David asked, now 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 online banking to make life easy for you..."

SADLY, THIS IS NO LONGER AN UNUSUAL SITUATION

While this is a fictitious story – the situation David has found himself in is no longer rare.

We often get calls from local businesses that have found themselves compromised somehow (these are not existing clients we're protecting, I hasten to add).

The outcome is almost always the same – money has gone from the business bank account. Stolen.

9 times out of 10, the entry point is the same too. An email account somewhere in the business has been compromised in some way.

When you think about it, the very nature of email makes it the weakest point of any security setup. For many of us, it's both our greatest tool and most hated nemesis.

You have lots of staff, accepting hundreds of emails every day. And even the best email filters in the world can't stop clever hackers because they're constantly inventing new ways to get in.

All they need is one member of your staff to click one dodgy link. And that can give hackers enough access to start monitoring what the business is doing. From there, they can spot ways to access business funds.

If a hacker can control your email, they can usually access multiple other systems and applications.

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 scary 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 affected.

THE HASSLE

David slammed the phone down in anger. 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.

He'd looked at the email his operations manager had received from the supplier, with the new bank details.

It really 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 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 he'd need to apologize for by the end of the day.

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

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

He'd called his key supplier, and thankfully she was happy to wait *until 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 savings to meet the payment and the 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. It was unlikely anyone would be able to follow the payment chain to the end.

While holding, David had Googled for advice. 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 him.

David picked up the phone again and called his IT support company. If the bank couldn't help, then at least the IT support company would shed some light on the situation.

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 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 large amount to this supplier.

“So they registered a new domain name that’s 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. 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 and very clever.”

“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, it’s a tricky thing to spot.”

“Now, what we need to figure out is how they got into your email 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 cybersecurity experts. We did offer you some extra protection last year, but you declined it."

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

"No need for that... it'll never happen to us."

COMMON EMAIL SCAMS AND HACKS

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

Not enough businesses put in place a proactive, preventative security strategy until they've been hacked. That's like waiting until you've been robbed to put locks on the door.

There are lots of different types of email hacks. 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 hackers gain access to your email just once and create an email forwarder. Then, without your knowledge, all incoming email is forwarded to them. They might not be able to see every reply you send, but it's usually quite 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 some money.

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

Follow-up emails: Exactly as David's ops manager was fooled – the follow-up email is a clever trick. The hackers have to get the timing right for this. If they can send a follow-up email immediately after the real email, most people assume it's real.

Compromising a supplier's email: It doesn't have to be your business that gets hacked to lose money. If they can compromise your supplier's email 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 a hacker adjusted all of your invoices. So your customers were making payments, but not to your bank account.

Edited PDF: Many people think a PDF on an email is a safe document. But PDFs can be easily edited. We've heard of hackers intercepting invoice PDFs, editing them to change the bank account details, and then sending them to customers. This is a very clever hack because the person paying the invoice will typically have zero suspicion.

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

Social engineering: Once a hacker 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 normal patterns of behavior, they can leverage that. We heard of one company where the boss's email had been compromised, with an email forwarder set up. The hackers 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. "Lovely sunshine here. I forgot to pay an invoice before I went – can you pay this quickly, please?"

Inevitably, the staff didn't think twice.

In another example, the hacker 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 full access to the boss's email while he was sitting on the beach, unaware he'd been hacked.

Staying on that theme – if there was one thing we would enforce within every business we protect, it would be this: **Never let the boss break 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 the staff comply!

This sets up circumstances for easy fraud. Any hacker sitting monitoring email traffic will see this happening and know it can be leveraged.

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

1.7 billion

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

1,425%

Hackers make a lot of money from cybercrime, with a reported **return on investment of 1,425%!**

60%

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

There are loads of scary stats out there – just Google "email security stats" to see for yourself.

Now let's rejoin 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," the 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 robust checklist of things we will do to kick your hackers out and prevent them from getting in again."

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

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

David felt his body relaxing for the first time in 24 hours. Since he'd discovered the theft yesterday morning, it had consumed every moment of his attention.

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

He'd also decided to hire a new IT support company. They were a lot more focused on cybersecurity 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 were 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 email business accounts and forced everyone to change their password. There were a few grumbles, but the team could see why it needed to happen.

They also set up multi-factor authentication. "It's just like when you log in to your bank account," David explained to his staff.

"You use an app on your phone to confirm the login and prove it really 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 standard 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 set up a scanner so they'd be notified if an email forwarder was ever set up again. They also created a complete audit trail within Office 365 to help diagnose any future hacking attempts.

And 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 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," he explained.

"We don't want you and your staff to ever 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 toward it," the technician continued.

"They will soon forget the pain of this hack. If they see the ongoing extra security as an annoyance 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 and education for your 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 relaxed that he had an expert on his side, helping him get this sorted out properly.

YOUR 9 LAYERS OF SECURITY

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

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

Because plenty of tools are available to protect companies of every size, the trick – as the technician explained to David – is putting together the right blend to suit your business. 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 and 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 with your mobile phone, either by receiving a code or using an app to generate a code.

2 - Monitoring for unauthorized email forwarders: As David discovered, hackers could play a clever, long game just by accessing your email once. An unauthorized forwarder allows 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 a specific email backup, your emails are not being backed up and are not protected daily. Not many people realize this. Having a proper backup is critical, as it gives your IT support company many more options if you are attacked. They can completely reboot your email account, safe in the knowledge you won't lose a single email.

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

5 - Improved security endpoints: Endpoint security means 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. To encryption of the data on the device, meaning it's worthless to anyone that steals it. And even as far as banning USB devices (you can plug them in, but they won't work... meaning they can't do any damage).

6 - Office 365 advanced threat protection: Robust Microsoft protection working for you behind the scenes. Your IT support company should know the correct way to implement it for your specific setup.

7 - Awareness training: The weakest link in any email security setup is... the humans. Because emails can 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. There are some amazing 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 dodgy link to click. That pause can save you thousands of dollars and days of hassle.

8 - Cyber insurance: It could be worth taking out a cyber insurance policy if only to follow the basic standards laid out by the insurance companies. Their job is to reduce their chance of having to pay out, right? That means they're highly likely to know what '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: 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 by the boss. Because it's when the boss cuts corners that the chance of fraud jumps up dramatically; the weakest link is humans, remember. When it's the boss, and everyone wants to please them, it opens the window for fraud and encourages everyone to break the rules. Great leaders realize they need to act the way they want their staff to act… even if it's an inconvenience.

THE FUTURE

David laughed at the joke and 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.

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

A member of staff who really should be fired. A major customer service failing.

And David couldn't help but chip in with his hack story from a few weeks before. Told in great detail with all the embellishments.

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

He had a rapt audience. They jumped in with a load 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.

"For 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 up to date.

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

Now he knew that assumption was completely wrong.

Business owners and managers were so busy that they had to filter out a lot of the noise.

He realized cybersecurity 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 when a friend has been burglarized. And more insurance when someone they know well gets a severe illness.

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

WHO DO YOU KNOW WHO'LL BE COMPROMISED NEXT?

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

Someone you know will likely 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 they've been hacked. Understandably, they are reluctant for clients and peers to find out!

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

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. Contact us to discuss our customized cybersecurity solutions.

ABOUT YEO & YEO COMPUTER CONSULTING

Yeo & Yeo Computer Consulting is a leading IT services provider in Michigan. Our goal is to supply reliable technology solutions that keep Michigan's organizations moving forward. We partner with leading IT vendors – including HP, Fortinet, Ergotron, Lenovo, Microsoft, VMware, Veeam, Xerox, Sage, Barracuda, Acronis, Cisco and Duo – to provide innovative solutions across many industries.

With services including managed IT, cloud solutions, cybersecurity, VoIP, IT consulting, hardware procurement, business management software and more, you experience the strategic advantage of a single-source partner. Using these services, our industry-certified professionals develop customized IT solutions to meet clients' needs. From design and implementation to long-term support and maintenance, Yeo & Yeo Computer Consulting makes your IT systems work for you.

For more information:

Contact Us Online
Learn more at yeoandyeo-consulting.com
Email: info@yeoandyeo.com
Call 989.797.4075 | 800.607.1446

YEO & YEO
COMPUTER CONSULTING

Information provided by MSP Marketing Edge