GMA
GREGORY MICALLEF ASSOCIATES

EMAIL HIJACK

How hackers break into your email to plunder your business bank account. Businesses are under attack, every day...

and here's what to do about it

By Greg Micallef,
Gregory Micallef Associates (GMA)

EMAIL HIJACK

How hackers break into your email to plunder your business bank account. Businesses are under attack, every day…

and here's what to do about it

By Greg Micallef,
Gregory Micallef Associates (GMA)

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!

That money had been intended for a key supplier who still needed to be paid, meaning a total hit to his cash flow of more than £24,000.

How?
How??
How???

It wouldn't kill the business, but David knew it would make things very tough for a few months.

What would he tell the staff? What would he tell his wife?
The day had started off in a much more promising fashion...

After ten wonderful days in Cyprus with his family, David had gone to the office at 7am, keen to catch up on the hundreds of emails that inevitably waited for him.

As the owner and MD of a fast growing business, it was rare for him to be away from his email for more than a few hours. However, after a very busy period at work David had promised his family that they would be having a 'proper' holiday this year, meaning no phone calls and definitely no emails.

He'd checked in with his Operations Manager from the airport on his way home, two days ago. Knowing there were no major issues he needed to deal with David had felt relaxed, calm, refreshed, and keen to get back to work.

It took less than 20 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. He logged onto business banking and could see the payment had left the bank account.

Believing it to be a misunderstanding David emailed his supplier's MD to tell her when payment had been made.

Having made an early start herself, Lorrie was sitting at her desk when David's email arrived and promptly called him to explain that the payment hadn't been received.

David promised to look into it and rang off, that was when the dreadful feeling began 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, and 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. David checked the payment details against the invoice.

Oh...Wow!

The sort code and account number that the payment had gone to were completely different to the ones on the invoice.

The dreadful feeling in his stomach was getting stronger, as David pressed a button on his phone and called his Operations Manager.

It was a phone call he would never forget.

"Yep it's all sorted out," his Operations Manager had said. "I paid it the day after they emailed it through."

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

"Maybe they're checking their old bank account in error. I paid it to the new one as requested." answered the Operations Manager.

Wait...What was that?

“What new bank account?” David asked, now deeply alarmed.

“Oh, they’ve moved banks,” his second in command continued, “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.”

In just a few moments all thoughts of the relaxing family holiday he had just enjoyed were gone, the business was in trouble!

SADLY, THIS IS NO LONGER AN UNUSUAL SITUATION

Hello, my name's Greg Micallef. I'm a data security and IT expert, and the owner of Gregory Micallef Associates (GMA).

It saddens me to tell you that – while this is a fictitious story – the situation David found himself in, is no longer rare.

In fact, at least once a month our phone rings and it's a business that has found itself compromised in some way (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! Nine times out of ten, the entry point is the same. An email account somewhere in the business has been compromised.

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

You have staff accepting emails every day. 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 on one dodgy link... And that can give them enough access to start monitoring what the business is doing. From there they can spot ways to access business funds.

If a hacker can get control of your email they can usually go on to access multiple other systems and applications.

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. For now, let's return to David's bad day and see how his business has been affected.

THE HASSLE

After holding for 20 minutes then receiving the news he feared, David slammed the phone down, he was angry and frustrated! What was the point of having a Relationship Manager at the bank if he couldn't help him in an emergency? The Relationship Manager had even spoken to his immediate supervisor, but said there was nothing further the bank could do to help.

The bank had tried to get the money back from the account the payment had been sent to, without success. In their experience money is normally removed quickly and the bank account abandoned. It was unlikely anyone would be able to follow the payment chain to the end.

David looked at the email his Operations Manager had received from the supplier, paying particular attention to the new bank details. It really did appear to come from them.

The Operations Manager went through all mandates in the bank account, spending a lot of time phoning up suppliers to check details were correct. Whilst 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. There were whispers amongst employees of the business having all of its cash stolen. David knew he'd need to talk to them all this afternoon to reassure them.

He'd phoned his key supplier back, thankfully she was happy to wait until the end of the week for payment but David wasn't looking forward to telling his wife he needed to take £20k out of their personal savings. He had little choice, they had to make payment to the supplier and payroll on Friday. They'd both believed the days of emergency director's loans into the business were long gone.

David picked up the phone again, this time calling his IT support company. If the bank couldn't help, then at least the IT company would be able to 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 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 clearly been monitoring your email for a while and have spotted that you regularly pay a large amount to this supplier. They registered a new domain name that's really similar to your supplier's domain, but it has an extra character in it – look, there's an extra 'e'. Can you see it?" finished the technician.

David peered at the email address, good grief! The technician was right! He wondered if he would have spotted the difference himself... probably not, would he have even been looking for it?

"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" the technician added. "I feel so stupid," David said.

"Don't," the technician replied. "Lots of people fall for this especially when rushing, or at the end of a busy day or week. Did you know that most email attacks happen at the end of the week, in the afternoon?. It's a really hard thing to spot, and it is unlikely to be noticed if staff are not looking for it. Even then it can still be difficult."

"What we really 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," he concluded.

"Isn't this something you guys should have stopped anyway? You are my IT support company after all," asked David. There was a pause on the other end. Then the technician replied...

"Well, we're not really cybersecurity experts. However, I know that we did offer you some extra protection last year, unfortunately it was declined."

David thought hard…the technician was correct, he had dismissed the idea of extra protection, almost out of hand. He hadn't thought it a necessary expense at the time. In fact, he recalled the exact words he had used…"No need for that… it'll never happen to us."

David felt his face start to turn red, he should have taken their advice, at least looked into it.

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 and preventative security strategy until they’ve been hacked. That’s like waiting until you’ve been burgled 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 put in place 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 on a regular basis. 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 xyzzcompany.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: This is exactly how David's ops manager was fooled, the follow-up email is a clever trick. The hackers have to get the timing right for this, but if they can send a follow-up email immediately after the real email, most people just 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. Now flip that round, and imagine a hacker adjusted all of your invoices so that 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 on 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 information back to the hackers, on every button you press. 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 login.

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 holiday. That's a break in normal patterns of behaviour, 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. 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 ASAP please".

Without the correct training it is highly unlikely any member of staff would notice anything wrong.

In another example the hacker sent an email 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, gaining full access to the boss's email while he was 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 break protocol!

Before we re-join David's story, **here are some email hacking stats we have gathered:**

91%

of cyberattacks begin with a spear phishing email.

92.4%

of malware is delivered by email.

1 in 25

branded emails are a phishing email.

Did you know?

1 in 5 Small businesses will suffer a cyberbreach this year.

81% Of all breaches happen to small and medium sized businesses.

97% Of breaches could have been prevented with today's technology.

The average loss due a cyberbreach in the UK ranges from **£3,650** for a micro business, to over **£22,700** for larger companies. It can also have a negative impact on brand reputation.

THE FIX

"It's can be impossible to pinpoint the exact entry point into your email system," explained the new Security Specialist.

"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 stop your hackers, and others, compromising your system again."

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

David felt his body relaxing for the first time in 24 hours. He'd had a terrible night's sleep, getting home late and then waking from a nightmare, covered in sweat, at 4am.

Since he'd discovered the theft yesterday morning, it had consumed every moment of his attention. He just couldn't shake feeling unsettled.

Undeniably he'd got a lot sorted out – including reassuring his employees and promising training to ensure that they were, at least, as prepared as anyone could be. He'd also hired a new IT support company that were a lot more focused on cybersecurity than his previous company. When they said cybercrime was the number one threat to businesses like his, he believed them.

After all, he was the bearer of hindsight now.

Having spent his entire focus on resolving the security breach David's other work had begun to accumulate. He thought about the hundreds of holiday emails that were still waiting, how his staff had suffered already, and how they were going to have to suffer a little more disruption until this issue was fully resolved.

The new IT support company immediately logged everyone out of the business email accounts, requesting that everyone change their password whilst adhering to the new password policy put in place.

They also had multi factor authentication set up. "It's just like when you login 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 that immediately stops us from being an easy hack in the future".

The technicians investigated the email trail that had led to the hack, and quickly discovered an unauthorised 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.

The new IT support company 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 a full audit trail within Office 365, to help diagnose any future hacking attempts.

Next 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 that really should addressed.

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

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

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

“They will soon forget the pain of this hack, and if they view the ongoing extra security as an annoyance that’s holding them back, they will not take it seriously. That could leave you even more exposed than you were before.”

“Together we’re going to find the right balance of security and education for your business,” added the security expert.

David scribbled notes on his pad, as the technician laid out the many different options available to him.

Even at this early stage David was able to identify which security measures would work well and which would hinder his employees.

For the first time since returning to work David started to feel a little more relaxed. He had an expert on his side, helping him to resolve this security crisis properly and ensure that the risk of this happening again is minimised.

YOUR 10 LAYERS OF SECURITY

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

However, they'd also struggle to do business and remain productive.

There are plenty of tools available to protect companies of every size. The trick, as the security expert explained to David, is putting together the right blend to suit your business, ensuring you are protected without tying your hands.

Here are the 10 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 starting point of 'best practice' that the average business should pick and choose from, using expert help for guidance.

1 - Multi-factor authentication: The most simple and effective way to prevent unauthorised logins. Every time you login 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. To counteract a new crime called 'simjacking', where someone clones your phone number to their sim card to intercept your multi-factor authentication alerts, there is also the option of using special devices you plug-in to your laptop.

2 - Monitoring for unauthorised email forwarders: As David discovered, hackers can play a clever long game, just by accessing your email once. An unauthorised 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 specific email backup, your emails are not being backed up, and therefore are not protected on a daily basis. Not many people realise this. Having a proper backup is critical, as it gives your IT support company so many more options in the event you are attacked. They can completely restore your email account from the backup, giving you the safety net of knowing you will not lose all your emails.

4 - Artificial Intelligence (AI) screening of emails: Let's say you have a 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 change in behaviour, and investigate the email further. These systems can be very clever at spotting potentially dodgy emails.

5 - Improved security endpoints: Simply put this means protecting a network when it is being accessed remotely and there are many different ways to do this. From enhanced security on each device to prevent it being used for suspicious activities, to encryption of the data on the device, meaning it's worthless to anyone that steals it. This can go 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: You want this! It's 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...us, the humans. Emails can still get past all of the defences I've already listed. The last line of defence (and frankly, the best) is the human looking at an email with suspicion.

7 - Awareness training cont: There are some amazing awareness training courses available, delivered online so your team don't have to go anywhere. They're not boring or full of tech-speak, instead they are designed to be fun, informative, and above all, to make your staff pause when they're sent that dodgy link. That pause can literally save you thousands of pounds, and days of hassle.

8 - Cyber Essentials: This isn't just a piece of red tape. I truly believe this course and accreditation will become compulsory for businesses in the years ahead, and quite right too. Cyber Essentials is designed to help and protect your business. Remember I said earlier that cybercrime is the biggest threat to businesses today. Doing the Cyber Essentials course helps you to get your business in the right mindset, and put in place the right level of protection. Increasingly, bigger businesses are demanding their supply chain has it.

9 - 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. 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.

10 - Set up business processes and make them the culture: Set up internal processes, if you have an internal process for approving payments, it needs to be followed every time, no exceptions. When corners are cut the chance of fraud jumps up dramatically.

Real security change is implemented from the top of the business down. Employers, supervisors, and managers need to lead by example, because great leaders know that they need to act in 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.

Their partners 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 business was great, they started swapping stories. David couldn't help but chip in with his hack story from a few weeks before, telling his tale in great detail.

The discovery. The hassle. The fix. How, weeks later, his cash flow was just starting to recover. David now knew the business would be fine, but wanted his friends to avoid the situation he had found his company in.

He had a rapt audience, his friends jumped in with lots of questions. David listened to them discussing the situation and remembered something his new security specialist had told him...
"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. He'd read business articles over the years about cybersecurity, but had assumed hackers wouldn't be interested in a business like his.

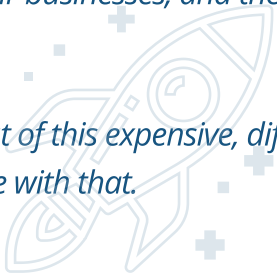
Now he knew that assumption was completely wrong.

Whilst the attack on his business had proved costly and as a result productivity dropped, the business had ultimately been saved. David felt fortunate after he had learned it was not something every attacked business could do, and even more lucky that the breach hadn't been bad enough to impact the brand reputation of the company.

As a result of his experience 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 burglar alarms when a friend has been burgled, and more insurance when someone they know well gets a serious illness - this group of friends were already considering the implications of an email hijack for their businesses, and the wider cybersecurity question.

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



WHO DO YOU KNOW WHO'LL BE COMPROMISED NEXT?

Whilst this is a fictitious story, the situation David found himself in is no longer rare.

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 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 afterwards. 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 and 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 fully protected with the correct layers for your specific situation, my team and I would love to help you.

More and more owners and managers are waking up to the risks and putting in place appropriate preventative measures.

This is how you can get in touch with us:
https://www.gmal.co.uk/
sales@gmal.co.uk
020 8778 7759

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

Thanks for reading.

GMA
GREGORY MICALLEF ASSOCIATES

YOUR EMAIL BEING HACKED IS YOUR WORST NIGHTMARE

91% of cyberattacks start with an email.

These aren't the young, moral hackers of the 80s and 90s who were breaking into systems just for the challenge.

Today it's a highly organised and lucrative crime. Using smart, automated tools constantly testing every business's armour. Looking for just one tiny crack in their defences to let them get in.

Their favourite access point is your email.
With a little patience and some smart thinking, 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 cybersecurity concepts in a way that anyone can understand.

This book also provides you with a checklist of 10 powerful defence weapons. So you can design the perfect blended security setup for your business.

Author **Greg Micallef** is an acknowledged data security expert, and owner of **Gregory Micallef Associates (GMA).**
Learn more at https://www.gmal.co.uk/contact/