# EMAIL HIJACK

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

Every day, every single business is being targeted...

**and here's what to do about it**

SWITCH MY SERVER

# SADLY, THIS IS NO LONGER AN UNUSUAL SITUATION

It's becoming increasingly alarming how many businesses have been hacked and found themselves compromised in some way.

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

Email hacking is 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 in. With a little patience, and some smart thinking, your email can provide direct access to the contents of your business's bank account.

**Don't let hackers break into your email and plunder your business bank account**

Here you'll find the most common email hacks and our checklist of 10 powerful defence weapons. Read our guide to design the perfect blended security setup for your business.

# COMMON EMAIL SCAMS AND HACKS

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

Not enough put in place a proactive, preventative security strategy until they've been hacked.

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.

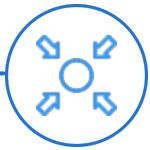
**Spoofed emails:** One scam is to buy a domain name that's very similar to real domain used by a supplier. So your supplier might use xyzcompany.com. And the hacker buys xyzcommpany.com. An extra character can often go unnoticed. Another trick would be to buy a domain with a different extension, such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

**Follow-up emails:** 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 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. Actually, flip that round, 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 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 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 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. Because 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. 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 ASAP 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 themselves full access to the boss's email while he was sat on the beach, unaware he'd been hacked.

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

**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


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


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

# YOUR 10 LAYERS OF SECURITY

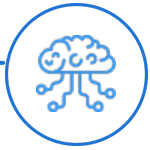
## If every business used every possible layer of email security, they'd reduce their chances of being hacked down to just 1% or 2%.

Here are 10 layers of email security we consider for clients we're protecting. Selecting the right variation to suit their business.

**1 - Multi factor authentication:** The simplest, and most effective way to prevent unauthorised logins. When you login to your email (or any other system) you have to confirm it's you, on a separate device. 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 plugin 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 so 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 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 change in behaviour, and investigate the email further. These systems can be very clever at spotting potentially dodgy emails from the tiniest symptoms.

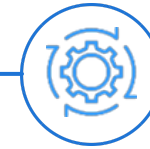
**5 - Improved security endpoints:** This is when each computer you use to access email is locked down and protected. There are many different ways to do this. From enhanced security on each device to prevent it being used for risky activities. To encryption of the data on the device, meaning it's worthless 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:** This is robust Microsoft protection working for you behind the scenes. But your IT support company has to 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 defences I've already listed. The last line of defence is the human looking at an email with suspicion. There are some amazing awareness training courses available. They're delivered online so your team don't have to go anywhere. They're not boring, 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 literally save you thousands of pounds, and days of hassle.

**8 - Cyber Essentials:** This isn't just a piece of red tape. We believe this course and accreditation will become compulsory for businesses in the years ahead. And quite right too. Cyber Essentials is designed to help your business and protect it. Remember I said earlier that cyber crime 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:** If you have an internal process for approving payments, it needs to be followed every time. No one should cut corners. When they do, the chance of fraud jumps up dramatically.

Processes need to be created and communicated on the implications of fraud. AND

**At Switch My Server, we do preventative work to stop email hacking 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. 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:


- craig.boddy@switchmyserver.com
- 01709 460333


Thank you for reading.


Craig Boddy
Switch My Server