EMAIL TAKEOVER

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

Every small to medium-size business is under attack, every day... and here's what to do about it.

idea LOGICAL

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 $20,000 stolen from his business bank account.

And because that money had been intended for a key supplier that still hadn't been paid, a total hit to his cash flow of more than $40,000.

How?

How?

How???

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

What would he tell his staff?

What would he tell his wife?

Today had started off a lot more promising...

After 10 wonderful days in Cyprus 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 Managing Director of a fast growing business in the GTA, 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 had 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 key supplier had 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. So he emailed his supplier’s finance director back to tell her when payment had been made.

She’d made an early start to Monday as well, as she called David 5 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 5 days ago, and hadn’t bounced back. That was when he thought to check the payment details against the invoice.

Oh. Wow.

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

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.

“Yep it’s all sorted out, mate,” 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. 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 bank mandate to make life easy for you...”

Email is an essential business tool — and that's exactly what makes it risky.

Before we continue, a brief pause.

The story you're reading is fictional, but the situation David ends up in is not.

At Idealogical, we support organizations across the Greater Toronto Area with IT and cybersecurity. And regularly, we hear from businesses that are calling because something has already gone wrong — not clients we're actively protecting, but teams reaching out after the damage has been done.

Almost every time, the result is the same: money has been taken directly from the business bank account.

In most cases, the starting point is also the same. An email account somewhere in the organization has been compromised.

Email is an essential business tool — and that's exactly what makes it risky. Teams move quickly, inboxes fill up fast, and even strong security filters can't stop everything. Attackers know this. They're patient, adaptable, and very good at making malicious messages look legitimate.

All it takes is one convincing email and one moment of distraction.

That single click can give an attacker the ability to quietly observe what's happening inside a business — who pays invoices, how approvals work, and when money moves. From there, financial fraud often follows.

And once an email account is compromised, attackers can usually go further. Many systems rely on email for password resets and account access. What feels convenient in daily work can quickly become a serious vulnerability.

In a moment, we'll explain the most common email-based frauds we see and how they unfold. But first, let's return to David's day — and walk through what happened when it all started to unravel.

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.

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 operations manager and called him stupid. In front of the other staff. That was a big mistake he'd need to apologise for by the end of the day.

Now the operations manager was fuming at his desk, going through all mandates in the bank account, and phoning up 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. There were whispers going round of the business having all its cash stolen, and them not getting paid. David knew he'd need to talk to them this afternoon and reassure them.

He'd phoned his key supplier, and thankfully she was happy to wait till the end

of the week for payment. She was certain that the bank details change email hadn't been sent by them.

David wasn't looking forward to telling his wife he needed to take $40k out of their personal savings in order to meet that payment, and then payroll on Friday. They'd both believed the days of emergency director's 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 really 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 the payment had been authorised by his business, the bank didn't have any legal obligation to refund him.

The online banking system alerting his ops manager to the account name not matching the payment details might have stopped the fraud.

But how often did someone just tick a box and click 'next' when doing something online they did all the time?

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 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 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. Good grief. The technician was right.

"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 really hard thing to spot.

"Now, 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."

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.

"We did offer you some extra protection last year, but you declined it."

David thought hard... and them 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.'

Too often, real protective measures only get put in place after an incident has already happened.

Common email scams and hacks

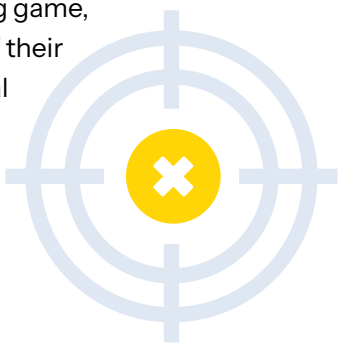
For most businesses, email security isn't something they worry about — until it suddenly becomes impossible to ignore.

Too often, real protective measures only get put in place after an incident has already happened. It's the digital equivalent of installing locks after a break-in has occurred.

There are many different ways email accounts can be compromised. The examples that follow are the ones we see most often — either first-hand, or shared through our wider network of cybersecurity partners.

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. This is even easier for them using AI tools. 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 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 (look at how many Ms there are in the middle of the word 'company'). 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 operations 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 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 it's an interruption to 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 in Cyprus. 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.

One pattern comes up again and again.

Nearly every organization has processes designed to prevent fraud — approval steps, payment controls, checks and balances. But those processes can unravel quickly when urgency enters the picture.

An executive sends a quick message asking for an immediate payment. The request looks legitimate. The tone feels familiar. And the team responds — doing what they believe is expected.

From an attacker's perspective, this is an opportunity. Anyone quietly monitoring email traffic can see how exceptions are handled and where rules bend. That insight is often all that's needed to take the next step.

Before we re-join David's story, here are three cyber security stats we have seen:

- **There are 500,000+** new malware samples detected every day
- **Two thirds of companies** have experienced a data breach… many are the result of poor email security
- **90% of breaches** involve social engineering

There's no shortage of statistics showing how common email-based attacks have become. The numbers are easy to find. What matters more is how consistently the same weaknesses show up across otherwise well-run businesses.

Now, let's return to David — just as he brings in outside help to deal with the email compromise and understand what went wrong.

The fix

"It's sometimes impossible to pinpoint the exact entry point into your email system," the 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 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 cyber security, as it's such a fast moving world. But what we're going to do 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. He'd 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 attention.

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

He'd also decided to hire a new IT support partner. They were a lot more focused on cyber security than his previous company. And he believed them, when they said cyber crime was the number one threat to businesses like his.

Pity the hundreds of holiday 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 partner immediately logged everyone out of their business's email 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 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 partner 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 unauthorised email forwarder. 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 a full audit trail within Microsoft 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 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. 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 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.

What matters
is choosing the
protections that make
sense for how your
business operates.

Your 10 layers of security

If a business layered every possible email security control on top of one another, the risk of being compromised would drop sharply.

But day-to-day work would also become very difficult.

The goal isn't maximum security at all costs. As the technician explained to David, it's about balance — putting the right mix of protections in place so the business is meaningfully protected, without grinding productivity to a halt.

There's no single solution that works for every organization. What matters is choosing the protections that make sense for how your business operates, with expert guidance to help you avoid unnecessary complexity

These are the 10 key layers of email security we typically consider when advising clients. This isn't an exhaustive list, and not every business needs every item. Think of it as a practical starting point — a set of best-practice options to select from, not a one-size-fits-all prescription.

1 Multi-factor authentication

This is one of the simplest and most effective ways to prevent unauthorized access. Logging in requires more than just a password — usually a confirmation on a separate device, such as a phone or a physical security key. It adds a small step for users, but dramatically reduces the risk of account takeover.

2 Monitoring for unauthorised email forwarders

As David discovered, email breaches don't always cause immediate damage. Sometimes attackers play a long game. By quietly adding forwarding rules, they can monitor messages and learn how a business operates.

3 Proper email backup

Many businesses assume their emails are fully backed up — but unless specific backups are in place, that may not be true. Proper email backup gives IT teams options during recovery, allowing accounts to be reset or rebuilt without losing critical communications.

4 AI screening of emails

Modern tools can spot subtle changes in behavior that humans might miss — small shifts in writing style, sender patterns, or context. These systems don't replace human judgment, but they add an extra layer of scrutiny that can catch emails that look legitimate at first glance.

5 Improved security endpoints

Email security doesn't stop at the inbox. Laptops and phones need to be protected too. That can mean device encryption, restrictions on risky activity, and controls that prevent harmful peripherals from being used. The goal is to make stolen or compromised devices far less useful to an attacker.

6 Advanced Microsoft 365 protections

Microsoft provides strong security tools built directly into its platforms — but they need to be configured correctly to be effective. When implemented properly, these protections work quietly in the background to reduce exposure without disrupting daily work.

7 Awareness training

Even with strong technical controls, some threats will still reach people's inboxes. That makes human awareness the final — and often most valuable — line of defence. The most effective training isn't technical or intimidating. It's practical, engaging, and focused on helping people pause and think before clicking.

8 Cyber essentials

This isn't just a compliance exercise. It's a structured way for organizations to build baseline security habits and improve decision-making. Increasingly, larger organizations expect their partners and suppliers to meet these standards as well.

9 Cyber insurance

Cyber insurance continues to evolve. While coverage varies, insurers tend to define clear expectations around basic security practices. Following those expectations can help strengthen an organization's overall posture — regardless of whether a claim is ever made.

10 Clear processes — followed consistently

Controls only work if they're followed. Payment approvals, verification steps, and escalation processes need to apply every time — especially when it's inconvenient or urgent. When exceptions become normal, the risk of fraud increases sharply. Strong leadership means modelling the behavior expected of the rest of the organization.

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 horror stories.

A member of staff who really should be fired.

A major customer service failing.

An idiot client.

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 most 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 that assumption was completely wrong.

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

He realised 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 burglar alarms when a friend has been burgled. And more insurance when someone they know well gets a serious 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.

This is where Idealogical helps — putting preventative protections in place early.

Book a call with our team to talk through your risk exposure and preventative options.

idealogical.com
connect@idealogical.com
416-410-5030

Who will be compromised next?

While David's story is fictional, the situation he finds himself in is not.

Incidents like this are becoming increasingly common. There's a good chance that, over the next year, a business owner or manager you know will deal with something similar — even if you never hear about it.

That's not surprising. Most organizations are understandably reluctant to talk publicly about being compromised. Concerns about reputation, client confidence, and trust often keep these incidents quiet.

That silence, though, makes it harder for others to learn from what's happened.

From our perspective, the most frustrating part isn't the clean-up work that follows an incident — it's knowing that many of these situations could have been avoided with the right preventative steps in place. It's far better to make security decisions calmly and deliberately, rather than under pressure, after something has already gone wrong.

Taking a proactive approach also tends to be simpler, less disruptive, and far more cost-effective. There's less urgency, fewer compromises, and significantly less impact on the business and the people running it.

If your organization hasn't yet put the right protections in place for how you actually operate, help is available. More business leaders are starting to recognize the risks and take preventative action — not out of fear, but out of responsibility.

The goal isn't perfection. It's preparedness.

Your email being hacked is your worst nightmare.

Every day, every single business in the Greater Toronto Area is being targeted by hackers.

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 organized 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.

And their favourite access point is your email, because 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.

idea LOGICAL

idealogical.com