Email Invoice Fraud

Invoice fraud through compromised email accounts has surged in the past 18 months, rivalling ransomware as the biggest cybersecurity threat our clients face. These fraudsters use surprisingly simple and consistent methods, with losses often surpassing $100k. Here's how it works...

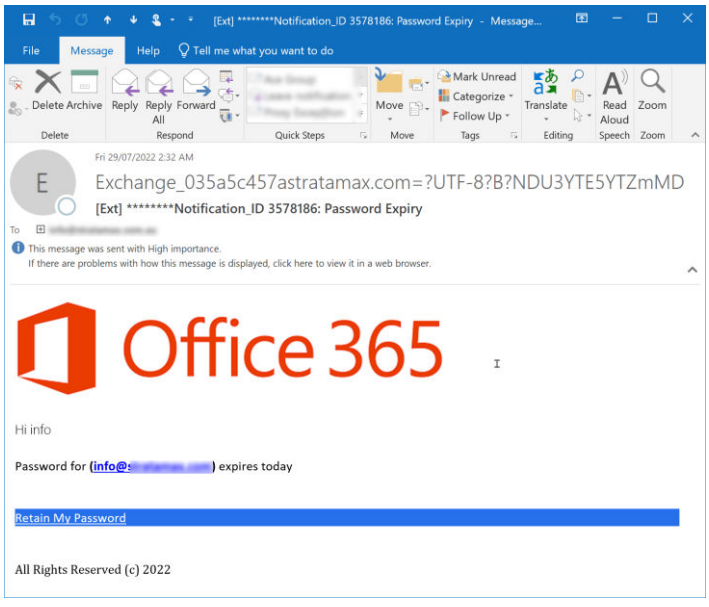
How does email invoice fraud occur?

Step 1. Hack your web-based email account

If your email is accessible via web browser, it can often be hacked — especially if you do not have some kind of two-factor authentication (TFA) in place. Hackers use a variety of methods to gain access to your email, including:

a) **Purchasing a database of compromised accounts.** These databases can be purchased on the dark web. They may include usernames and passwords for millions of users across a variety of platforms (e.g. Adobe, LinkedIn, etc.). Hackers breach platform, access the data, and then sell it to other hackers. People who reuse the same password are particularly vulnerable.

b) **Phishing attacks.** A hacker might send you a fake email asking you to re-login to your email account to verify something. The e-mail may look legit. The link in the email may lead to what looks like your provider's official website, but it's actually a lookalike "attack" website used to record the credentials you enter. The hacker will then use the credentials to log in to your email. Here is a screenshot of a phishing email I received this week:



c) **Malware.** A malware attack starts with an email that contains a link or an attachment. When clicked, it installs the hacker's software onto your computer. This software may allow the hacker to remotely track your keystrokes, monitor your activity, and otherwise snoop on you.

Step 2. Access your email account and create rules

Once the hackers have access to your email account, they will create forwarding rules that look for key words like "invoice" or "bank account." When triggered, it will forward a copy of the email to the hackers' email address. The same rule usually deletes the original forwarded email from the sent folder so you don't realised it's happened. The hacker then monitors these emails for the right criteria to move on to the next step.

Step 3. Adjust the invoice and set up a fake email address

When the forwarding rules deliver an invoice to the hackers, they will then use a PDF editor to change the details of the receiving account. They will also use a mail server to "spoof" the suppliers email address or register a fake domain that looks similar. A spoofed email will look like it came from the original sender of the invoice, but in fact it has come from somewhere else. An inspection of the email header would detect the deception, but this is too technical for most users.

Alternately, the hacker might register a domain similar to the supplier. For example, an email from accounts@abcplumbing.com might come from accounts@abcplumbng.com instead.

The hackers will then send the doctored invoice to the victim from the fake email address, banking on the likelihood that the victim won't know the difference and pay the invoice without question.

Step 4. Sweep the funds

If the victim pays the invoice, the funds will usually go to a compromised bank account set up in the name of a fake identity. The funds are then swept through a network and are very difficult to trace. Unfortunately, you are unlikely to recover these funds through the banking system — the funds have already left before the banks can to stop them.

How to protect your business

Email Protection – Two Factor Authentication

The simplest security measure to help prevent email fraud is to enable **multifactor authentication** or **two-factor authentication** (MFA/TFA) for your email account. This will involve the use of one or more authentication steps in addition to your username and password. Examples include an SMS, secure code generator, or biometric authentication like a fingerprint or face scan. Once enabled, MFA/TFA significantly reduces the risk of a hacker gaining access to your account.

Manual Verification

Offices need to implement stringent procedures to manually verify bank account details when setting up a **new supplier** or **dealing with changes** to account numbers and BSBs. There are multiple ways to do this, but regardless of the method, the details used to phone the supplier must come from a trusted third-party source and are not from the potentially compromised invoice itself.

Education

Safeguarding your business means providing general cybersecurity training for all staff. We recommend regular training in bite-size chunks to keep cybersecurity front-of-mind.

Cyber Hootl is one affordable product that offers this style of training. (insert link here). It allows you to configure the frequency of delivery. Most training sessions are just five minutes in length with follow up questions. The platform even allows you perform in-field tests by sending your team fake emails, complete with reporting on who clicks the links. This will help you identify potential knowledge gaps and follow up with additional training.

One free option is a free security newsletter called OUCH. It provides well researched and relevant articles with the latest on scams along with tips for keeping safe: www.sans.org/newsletters/ouch/

StrataMax Software Security

The last mitigation strategy to avoid invoice fraud is to lock down StrataMax access to your suppliers' BSB and account numbers, both for adding them and modifying them. Pay attention to software alerts or warnings for accounts that have been changed. Verify those changes before you make payment.