# CYBER SECURITY ISSUES FOR SMALL BUSINESS

Big business cyber for small & growing enterprises

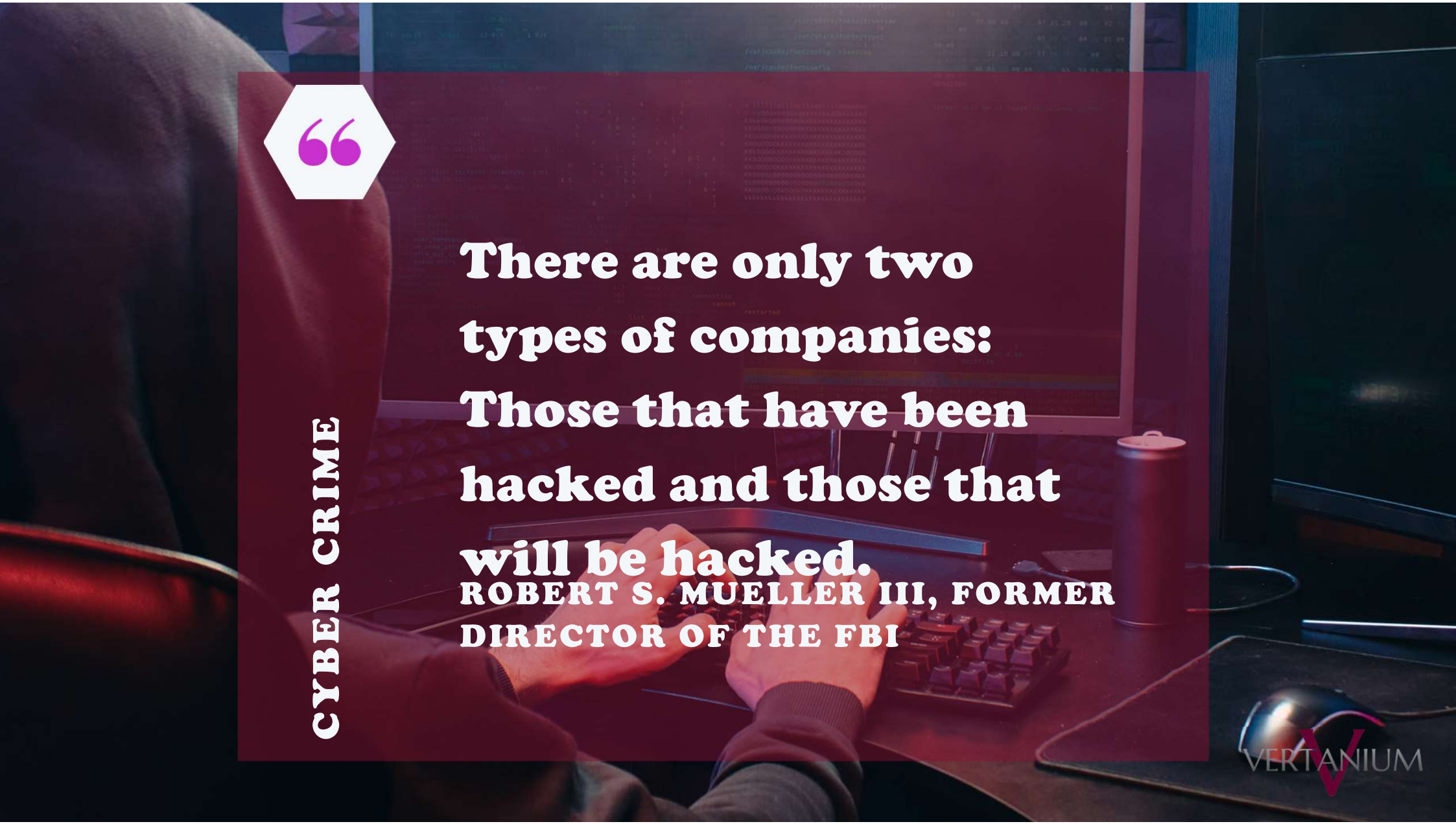
VERTANIUM

Rhonwyn Learner

Director

Matthew Bennett

Expert in Residence


CYBER CRIME
There are only two types of companies: Those that have been hacked and those that will be hacked.
ROBERT S. MUELLER III, FORMER DIRECTOR OF THE FBI
VERTANIUM

# REPORTED CRIMES BY TYPE

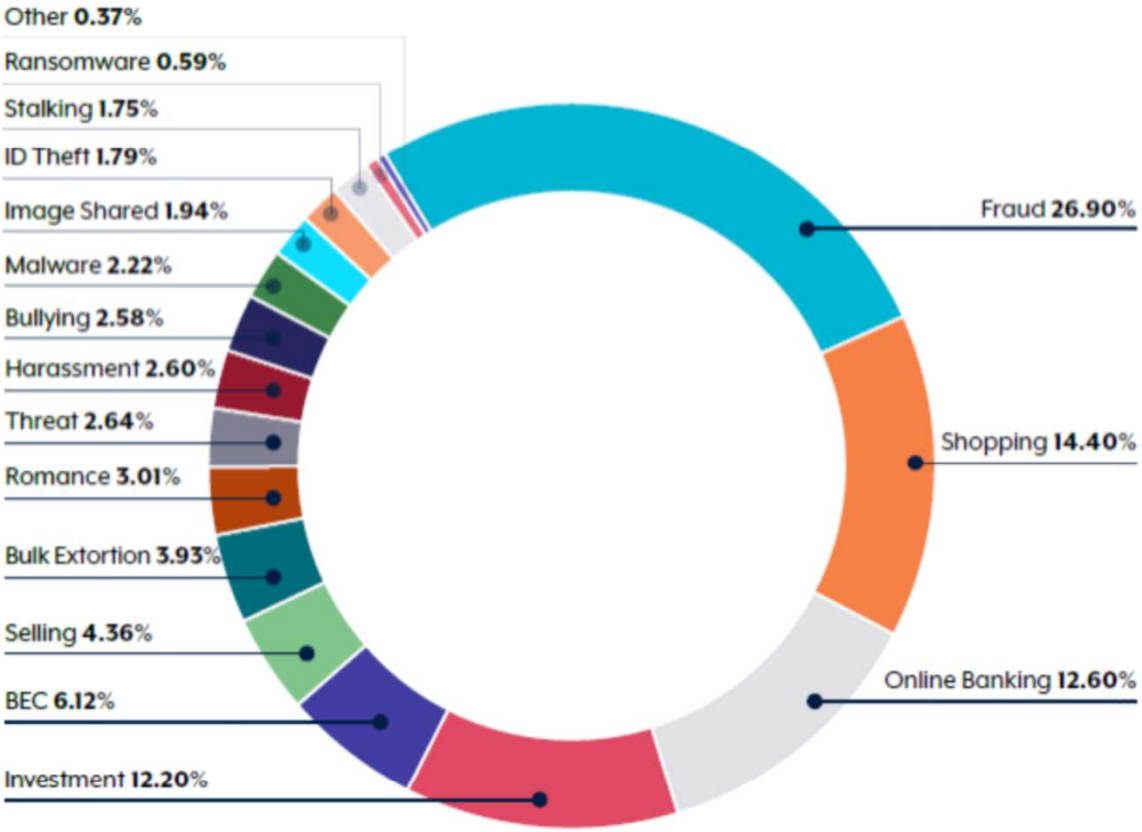



**Figure 3: Cybercrime reports by type for financial year 2021–22**

Source: ACSC Annual Cyber Threat Report 2021-22

VERTANIUM

# DIFFERENT TYPES OF ATTACKS

| | | |
|---|---|---|
| PHISHING | RANSOMWARE | MALICIOUS PROGRAMS |
| UNAUTHORISED ACCESS | MAN IN THE MIDDLE | DEEP FAKE AI |

# PREREQUISITES FOR PREVENTING CYBER ATTACKS

COMMITMENT FROM THE OWNER/S AND STAFF TO LEARN, APPLY AND MAINTAIN

SETTING A REALISTIC BUDGET ON ONGOING CYBER SECURITY PROTECTION INCLUDING MONITORING

HAVE A TRUSTED CYBER SECURITY PARTNER TO WORK WITH YOU AND YOUR IT TEAM/PERSON

CONSIDER INCLUDING PARAMETERS WITH SUPPLIERS AND SUBCONTRACTORS TO ALSO SHOW EVIDENCE OF MEETING MINIMUM CYBER SECURITY BENCHMARKS

ENSURE REGULAR TRAINING FOR YOU AND YOUR STAFF (OR SUBCONTRACTORS)

VERTANIUM

# WHAT HAPPENS WHEN YOU'RE ATTACKED?

YOU MAY EXPERIENCE A FORCED SHUT DOWN OR BE LOCKED OUT OF YOUR OWN SYSTEMS OR FILES.

A DATA BREACH WHERE THE PRIVATE INFORMATION OF YOUR CLIENTS, PARTNERS AND SUPPLIERS ARE LEAKED.

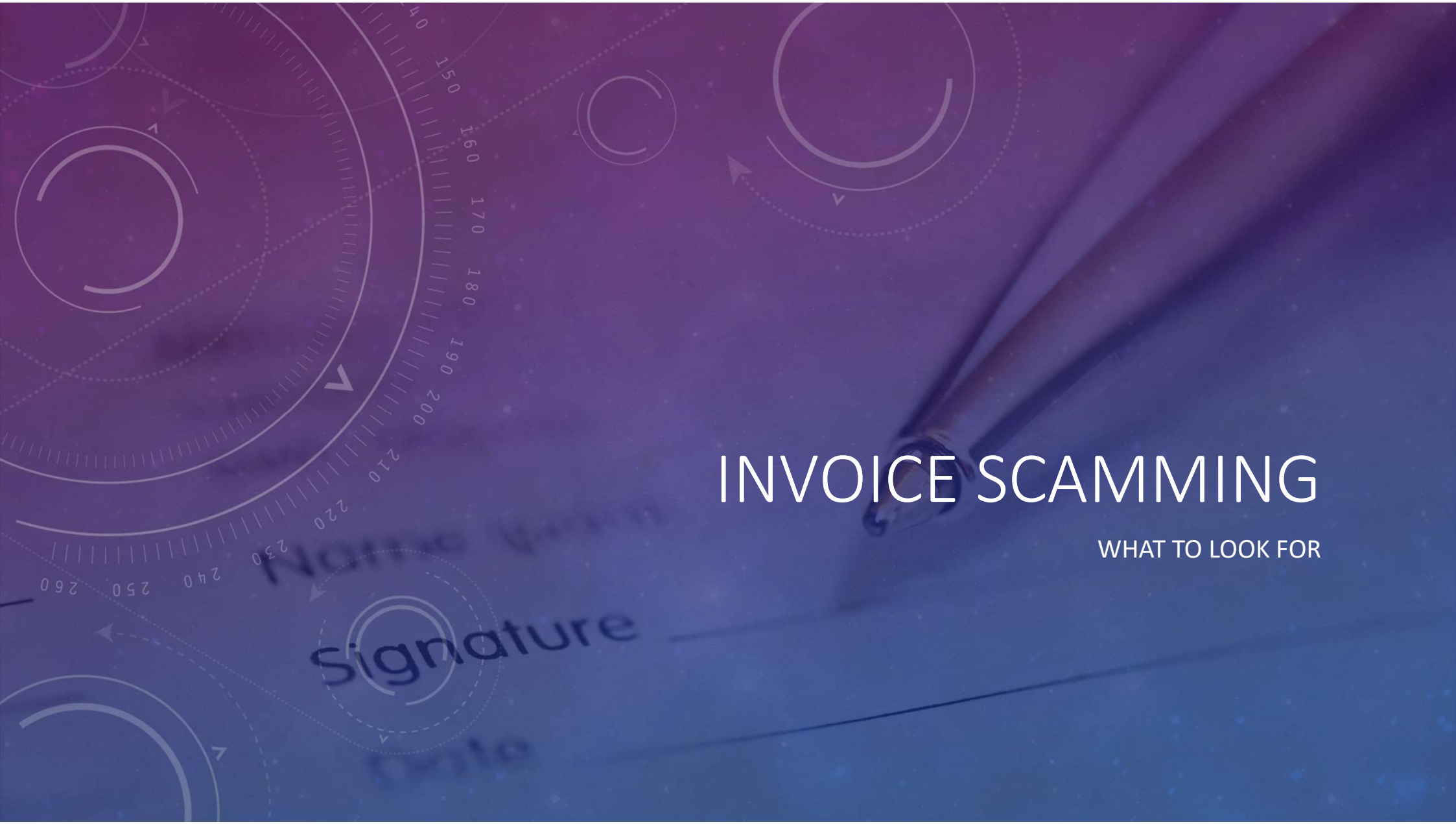
YOU COULD FACE FINES OR CIVIL ACTION.

YOU COULD LOSE YOUR GOOD REPUTATION AND BRANDING. THIS CAN BE CATASTROPHIC FOR SOME BUSINESSES, ESPECIALLY DIGITAL BUSINESSES.

LOSS OF REVENUE AND PRODUCTIVITY.

CAN'T PAY YOUR STAFF (INCLUDING YOU).

VERTANIUM




# INVOICE SCAMMING

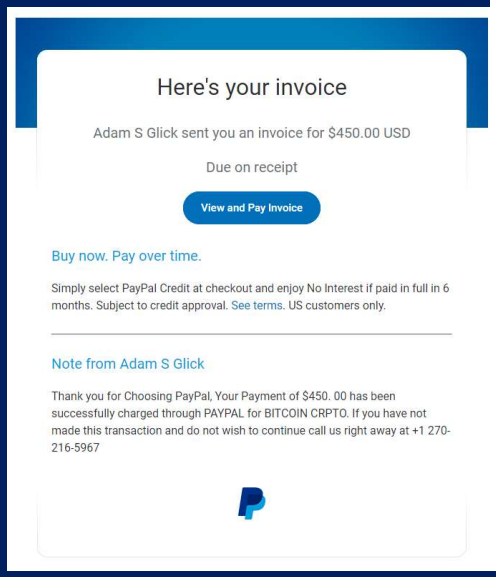
WHAT TO LOOK FOR

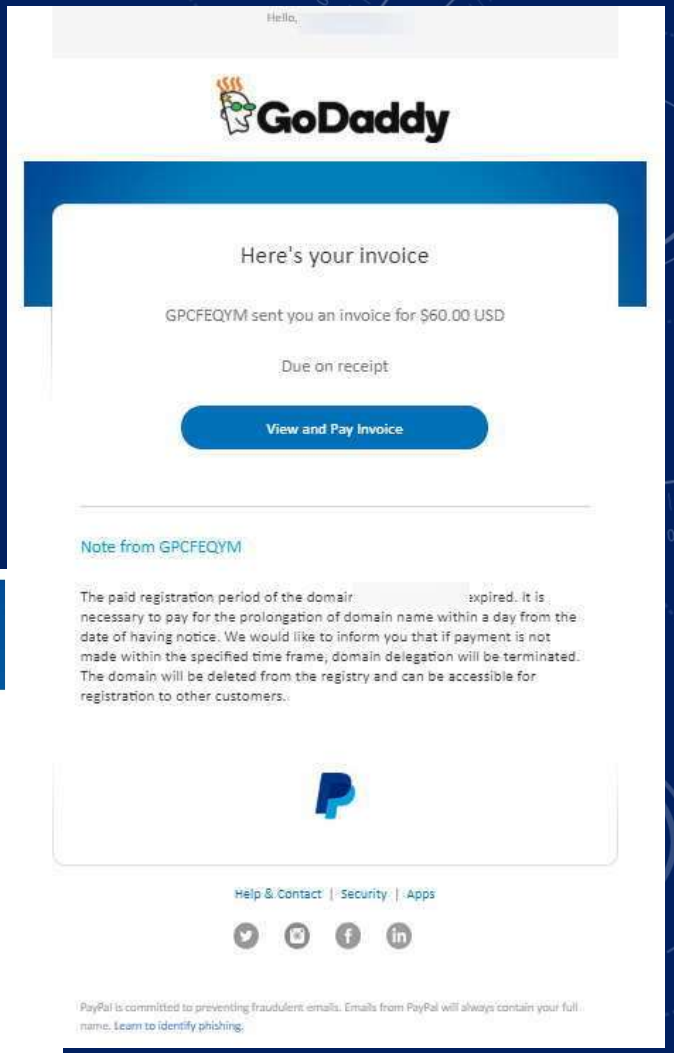
# WHAT IS INVOICE SCAMMING

Invoice fraud is a form of business email compromise which can result in enormous payouts for scammers. If a business processes hundreds or thousands of invoices each month, tricking you with a fraudulent email invoice can be quite simple.

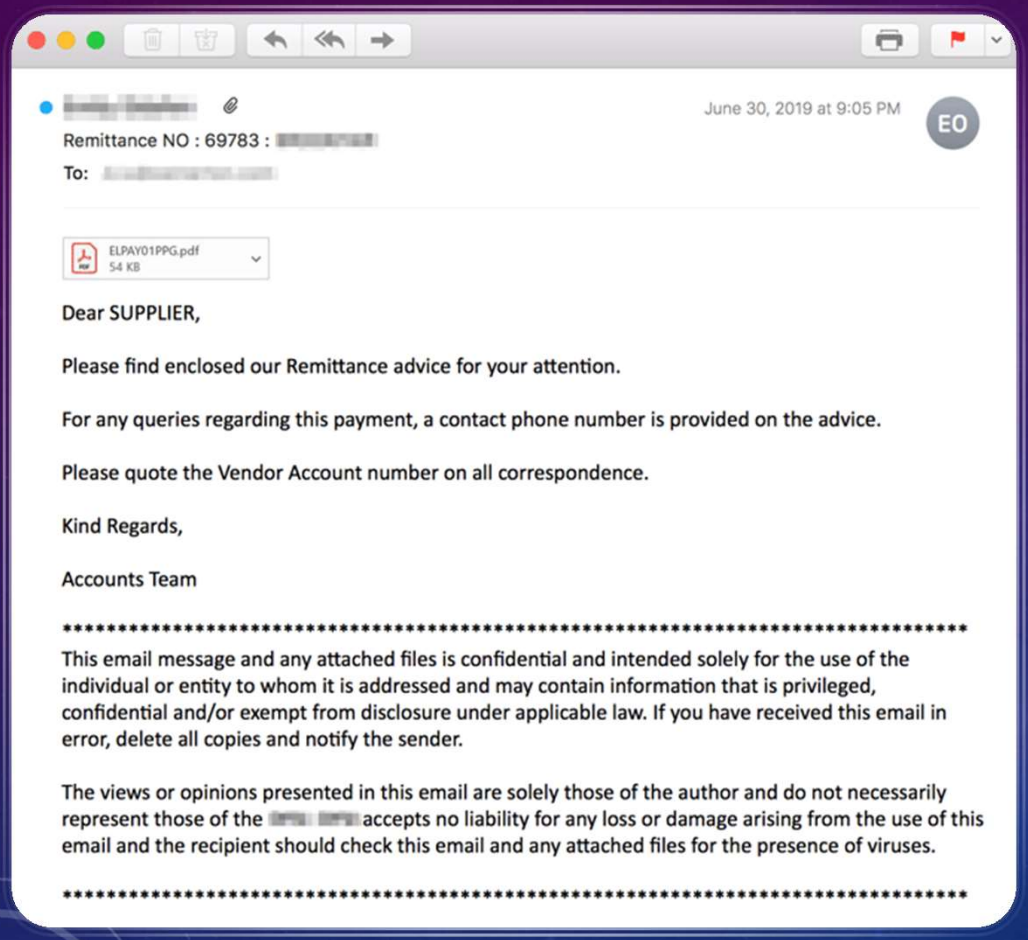
## What is business email compromise and how does it relate to invoice scamming ?

Formerly dubbed as Man-in-the-Email scams, BEC attackers rely heavily on social engineering tactics to trick unsuspecting employees and executives.




VERTANIUM



June 30, 2019 at 9:05 PM

EO

Remittance NO : 69783 :

To:

ELPAY01PPG.pdf
54 KB

Dear SUPPLIER,

Please find enclosed our Remittance advice for your attention.

For any queries regarding this payment, a contact phone number is provided on the advice.

Please quote the Vendor Account number on all correspondence.

Kind Regards,

Accounts Team

**********

This email message and any attached files is confidential and intended solely for the use of the individual or entity to whom it is addressed and may contain information that is privileged, confidential and/or exempt from disclosure under applicable law. If you have received this email in error, delete all copies and notify the sender.

The views or opinions presented in this email are solely those of the author and do not necessarily represent those of the accepts no liability for any loss or damage arising from the use of this email and the recipient should check this email and any attached files for the presence of viruses.

**********

# HOW IT WORKS: WHAT CLIENTS NEED TO LOOK OUT FOR

- Bogus supplier invoice that looks real with a different bank account
- Bogus supplier email address one single letter apart
- Altering a PDF invoice to change the bank account number for payment
- The sender asks for PII
- The invoice is for something you didn't purchase
- The email includes suspicious links
- The email links to a landing page of an illegitimate URL (hover)

VERTANIUM

# WHAT DO BUSINESS OPERATORS NEED TO LOOK FOR:

1. Be wary of emails that were unexpected when looking at invoices that are being sent

2. Look for red flags:
   - Red flag 1: A not-so-crisp logo
   - Red flag 2: Account numbers look different
   - Red flag 3: Contact info ever-so-slightly changed
   - Red flag 4: Invoices in even amounts
   - Red flag 5: Same numbers over and over

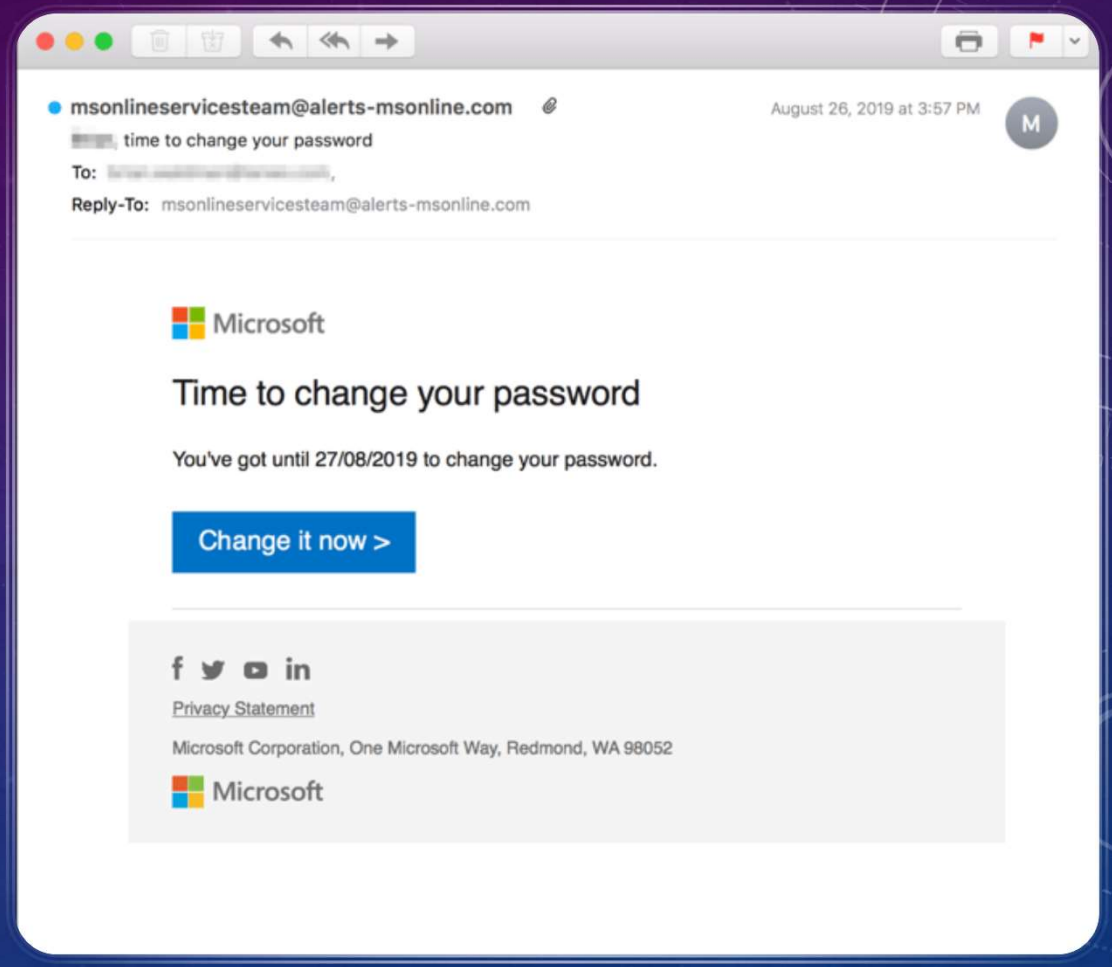
3. Never give out your personal identifying information unless you are certain who you are dealing with.

VERTANIUM

# WHAT DO BUSINESS OPERATORS NEED TO LOOK FOR:

4. Keep your business information safe. Beware of anyone asking you to 'confirm' your details and don't share you details unless you've checked the person you are dealing with is who they say they are.

5. Always exercise caution when receiving or downloading attachments or clicking links in emails, text messages or social media posts, even if they appear to be from someone you know.




VERTANIUM



# IF YOU DO NOTHING…

YOU'RE SETTING YOURSELF UP TO BURN MONEY

VERTANIUM

# GOOD FINANCE HABITS - INTERNAL PROCESSES

| | | |
|---|---|---|
| Verify Vendors | Verify Banking Details | Avoid emailing sensitive information |
| Implement “Fuzzy Matching” | Employ Automation | Initiate E-INVOICING |

VERTANIUM

# GOOD FINANCE HABITS - HUMAN ELEMENT

- Employ 3-Way Matching
- Track Invoice Activity
- Watch Threshold Invoice Amounts
- Regular staff and supplier training on internal policies and procedures
- Regular staff training on incident identification and response
- Provide regular updates on cyber alerts and attacks
- Foster positive work culture and moral

VERTANIUM


AI TOOLS FOR
SMALL BUSINESS
SPEED AND ACCURACY

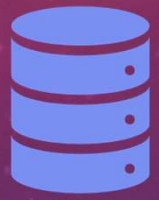
# WHY IS AI A THING NOW?

- Evolution in mathematics, AI algorithms and computer processing power
- Access to open-source AI instruments to integrate into commonplace digital programs
- Arrival of AI writers like Jasper, WriteSonic etc to evolution of ChatGPT release (more than just blogs)
- Floodgate of mass discovery into AI tools, including yourself
- Natural progression to AI tools being used for both attack and defence in digital security landacape

# TOP AI TOOLS FOR SMALL BUSINESS

- ChatGPT – research and writing most copy as well as mapping strategies and procedures for business
- GrammarlyGo – writing tool
- Midjourney – image generator
- Canva Magic AI – writing, image, design and other tools
- GPTBoss – ‘swiss army knife of AI’ as an ChatGPT alternative
- AgencyGPT - configure and deploy Autonomous AI agents to generate tasks to do, executing them, and learning from the results
- 60Sec.site – AI generated website ready to tweak and go live in minutes
- LimeCube – also creates AI generated websites = layout, theme, images and copy

# ADVERSARIAL ATTACKS ON BUSINESSES



**Poisoning Attacks -** modifying the training data resulting in a model trained on corrupted data

**Evasion Attacks -** manipulating input data to deceive the model into making incorrect predictions or decisions

**Generative Attacks -** generating new input data designed to deceive the machine learning model

# ADVERSARIAL DEFENSES FOR BUSINESSES

**Adversarial Training -** training machine learning models on clean and malicious data, which helps the model recognise attacks

**Model Diversity -** Using multiple models with different architectures and training data

**Input Validation -** Validating input data to detect any anomalies or malicious data

**Defence Mechanisms -** such as input normalization, feature selection, and outlier detection can also help to mitigate the risk of adversarial attacks

# COMPLETE CYBER SECURITY PROTECTION

THE PUZZLE IS INCOMPLETE WITH ONLY A FEW PIECES

VERTANIUM

# HOW DO WE START PROTECTING?

We can help with:

- Basic cyber training (live or online)
- Vulnerability Audits
- Foundation documentation for tendering and compliance
- And more…


VERTANIUM

# ADDITIONAL RESOURCES

- E-Invoicing developed by the ATO; access through your own bookkeeping program; https://www.ato.gov.au/business/einvoicing/what-is-einvoicing-/
- https://www.cyber.gov.au/ for up-to-date info on steps to protect
- Scam Watch by ACCC; https://www.scamwatch.gov.au/
- Grants:
  - Logan https://www.logan.qld.gov.au/grant-programs
  - Queensland https://www.business.qld.gov.au/starting-business/advice-support/grants/schedule

VERTANIUM

# BUSINESS BOOST GRANTS PROGRAM - OPEN

- Available funding is $10,000–$20,000 (excluding GST)
  - Applicants contribute an equal amount to the funding requested from DYJESBT (that is at least 50% contribution)
- This support includes funded activities in 3 project areas:
  - Future planning
  - Specialised and automated software
  - Planning and systems for staff management and development.

# BUSINESS BOOST GRANTS PROGRAM - OPEN

- To be eligible for this grant, your business must:
  - have between 2 and 19 employees (by headcount)
  - have an active Australian Business Number (ABN) and be registered for GST*
  - have Queensland headquarters*
  - be established and financially sound, experiencing growth and with a minimum turnover of $300,000 in the last financial year (2022–23)
  - have a publicly accessible web presence to identify business operations (e.g. business website and/or social media pages)
  - not have been approved for funding under Round 1 or 2 of the Business Boost grant program
  - not be insolvent or have owners/directors that are an undischarged bankrupt.

# Questions?

Email us at hello@vertanium.com

Connect with Rhonwyn on LinkedIn

VERTANIUM