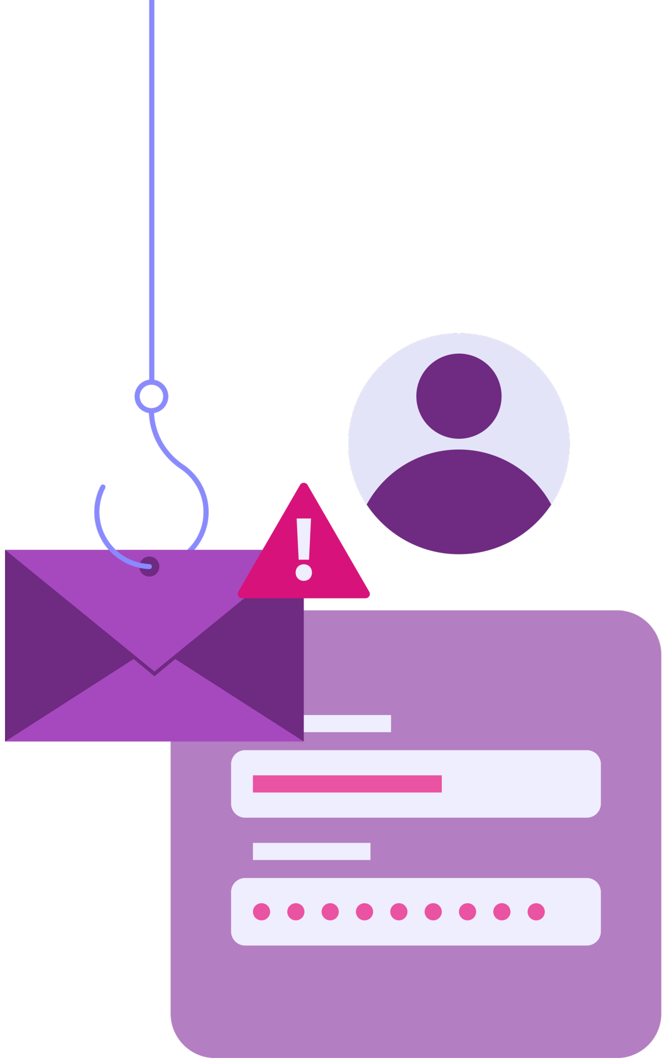
paymerang℠

The Evolving Landscape of Fraud Prevention:

Latest Insights and Strategies



Presenters

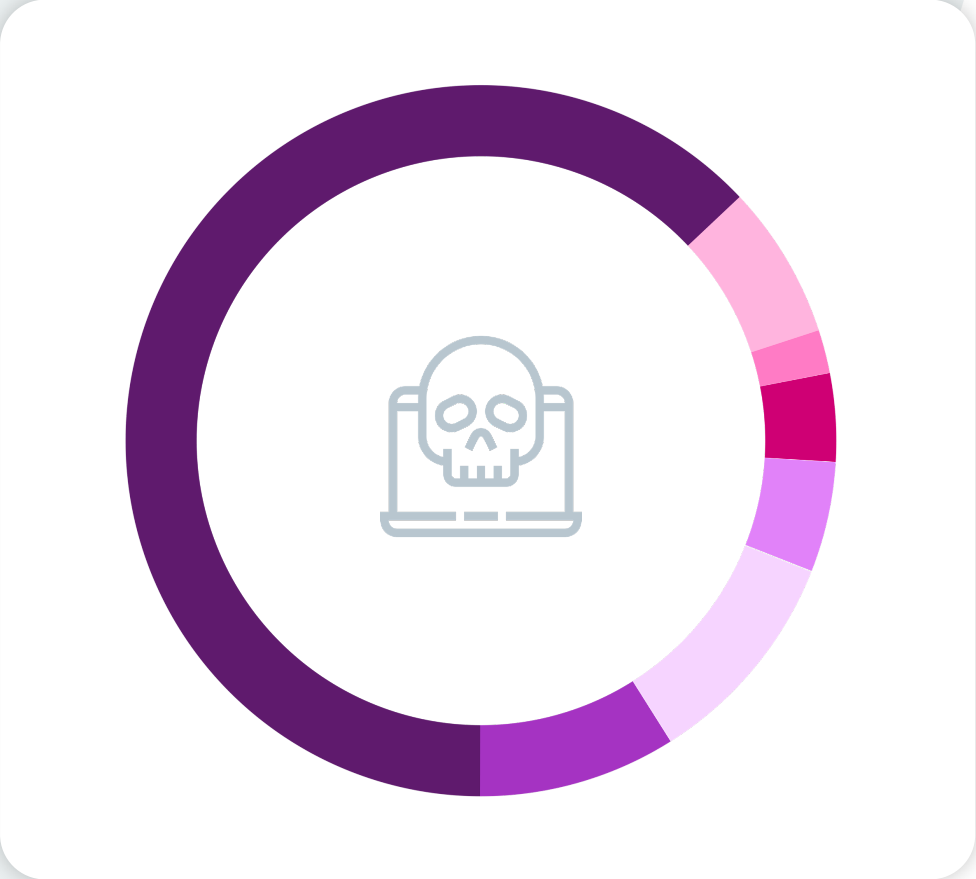
Sierre Lindgren

Fraud Prevention Manager

Michael Doerr

Vice President, Business Development

A matter of when, not if



Departments Most Vulnerable to Being Targeted by BEC Fraud

(Percentage Distribution of Organizations)

- ● 59% - Accounts Payable
- ● 10% - Treasury
- ● 7% - CEO, COO, CFO or other C-Suite Executive
- ● 12% - Procurement/Sourcing
- ● 2% - Human Resources/Payroll Dept.
- ● 1% Accounts Receivable
- ● 6% - Other

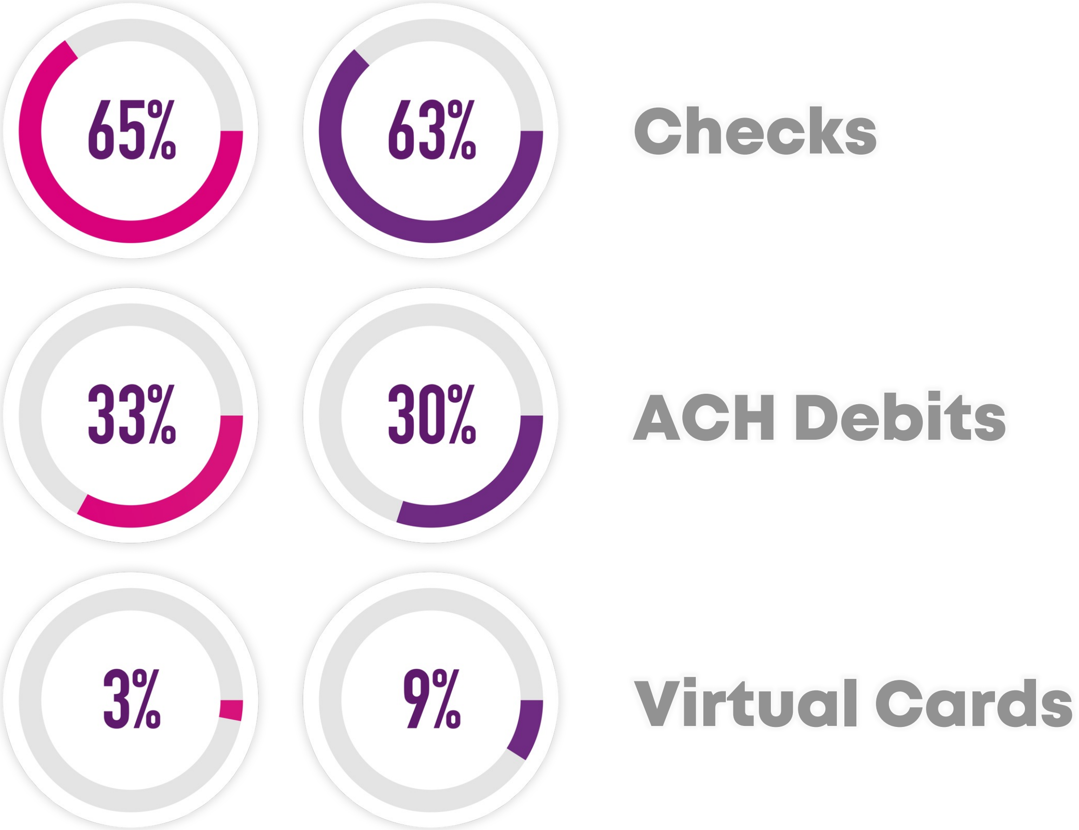
Source: 2024 AFP Payments Fraud and Control Survey Report

Payment methods impacted by fraud

Payment Methods Subject to Attempted or Actual Fraud

(Percent of Organizations)

● 2023 ● 2022



Source: 2024 AFP Payments and Control Survey Report

Checks are not a safe option

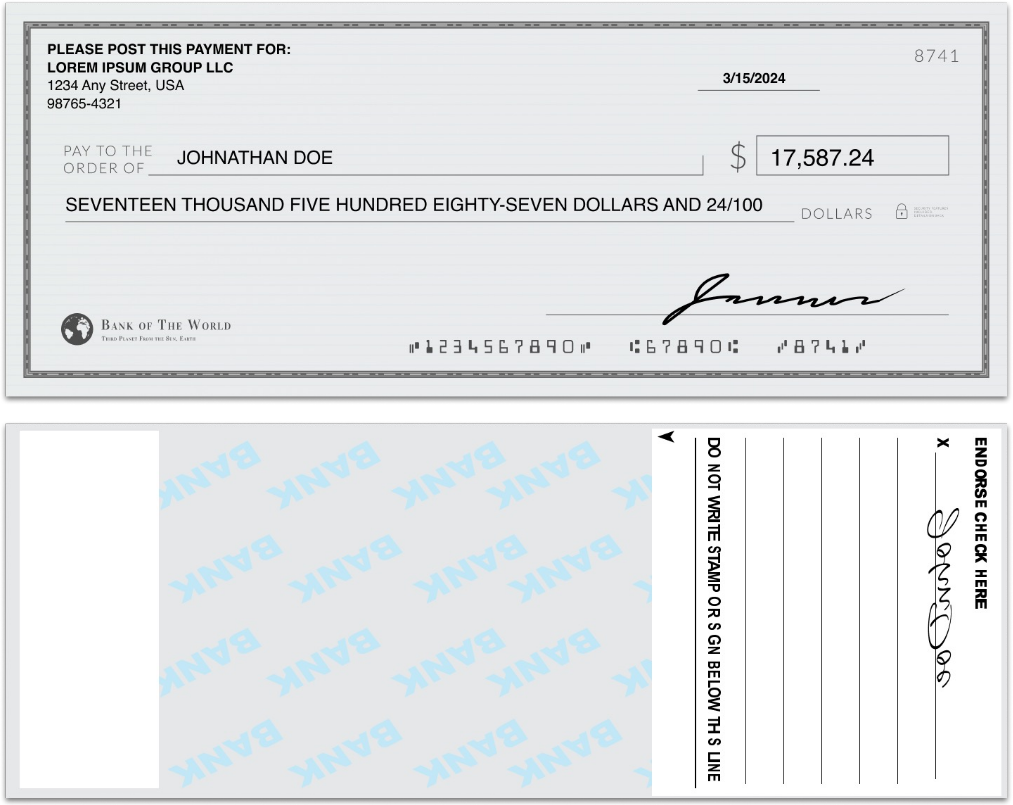
65%

IN 2023, 65% OF COMPANIES PAYING BY CHECK EXPERIENCED REAL OR ATTEMPTED FRAUD.

Source: 2024 AFP Payments Fraud and Control Report

Positive Pay

COUNTERFEIT



PLEASE POST THIS PAYMENT FOR:
LOREM IPSUM GROUP LLC
1234 Any Street, USA
98765-4321

8741

3/15/2024

PAY TO THE ORDER OF JOHNATHAN DOE $ 17,587.24

SEVENTEEN THOUSAND FIVE HUNDRED EIGHTY-SEVEN DOLLARS AND 24/100 DOLLARS

BANK OF THE WORLD

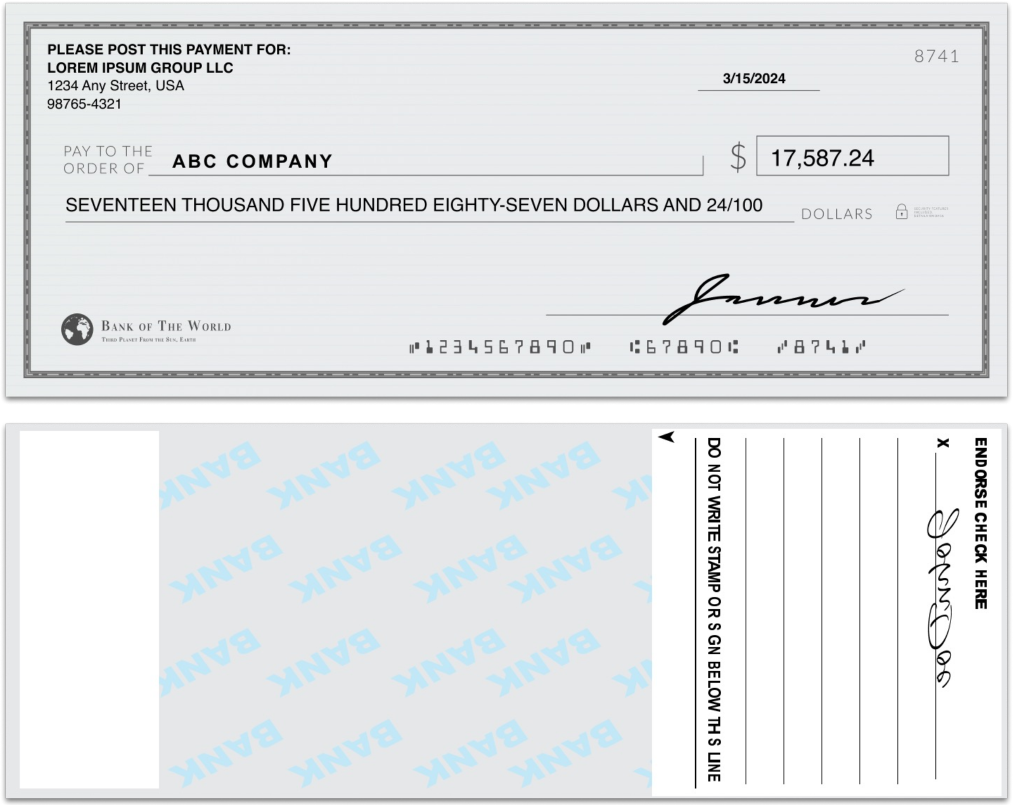
⑈1234567890⑈ ⑆67890⑆ ⑈8741⑈

ENDORSE CHECK HERE

x John Doe

DO NOT WRITE STAMP OR S GN BELOW TH S LINE

WITHOUT ENTRY



PLEASE POST THIS PAYMENT FOR:
LOREM IPSUM GROUP LLC
1234 Any Street, USA
98765-4321

8741

3/15/2024

PAY TO THE ORDER OF ABC COMPANY $ 17,587.24

SEVENTEEN THOUSAND FIVE HUNDRED EIGHTY-SEVEN DOLLARS AND 24/100 DOLLARS

BANK OF THE WORLD

⑈1234567890⑈ ⑆67890⑆ ⑈8741⑈

ENDORSE CHECK HERE

x John Doe

DO NOT WRITE STAMP OR S GN BELOW TH S LINE

Payments fraud

80%

OF ORGANIZATIONS WERE VICTIMS OF PAYMENTS FRAUD ATTACKS & ATTEMPTS IN 2023

Source: 2024 AFP Payments Fraud and Control Report

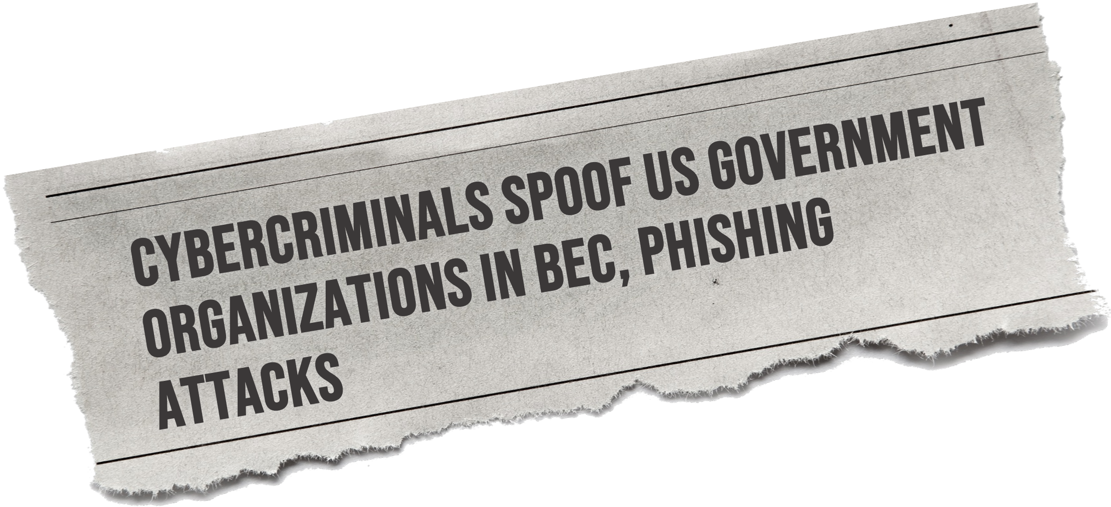
Business Email Compromise

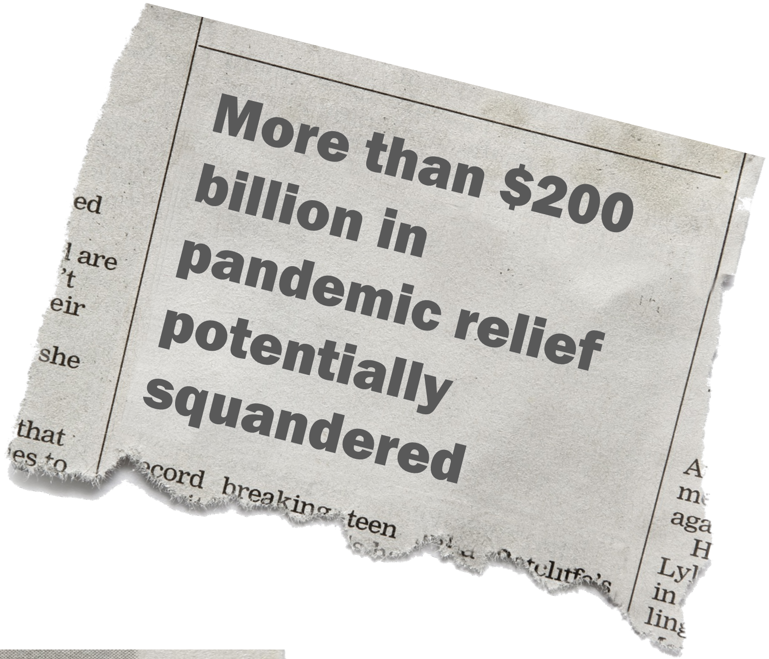
$2.9 BILLION

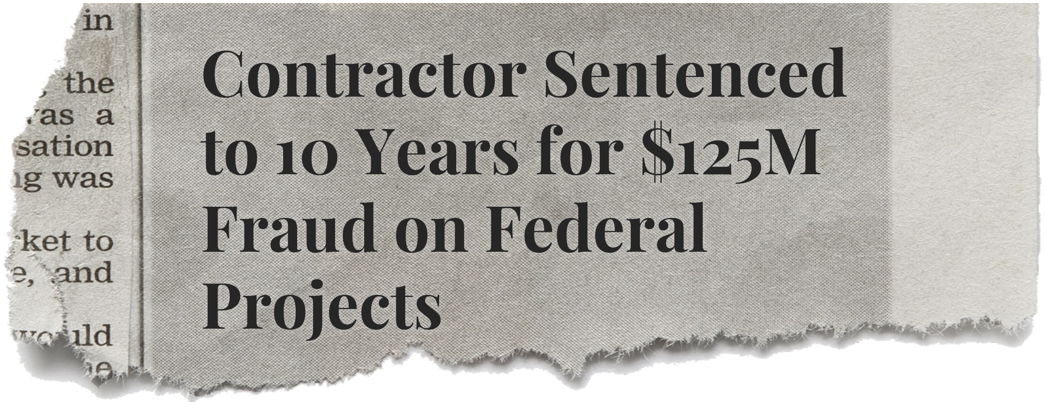
In 2023, the IC3 received 21,489 BEC complaints with adjusted losses over $2.9 billion

Source: FBI IC3 Report

Fraud in the news


CYBERCRIMINALS SPOOF US GOVERNMENT ORGANIZATIONS IN BEC, PHISHING ATTACKS


More than $200 billion in pandemic relief potentially squandered


Contractor Sentenced to 10 Years for $125M Fraud on Federal Projects

Key threats of fraud

ORGANIZATION

Fraudsters are increasingly professional in approach, even dividing their operation into different functions

COMPLEXITY & SPEED

Methods of fraud-attack and the associated techniques used are increasingly sophisticated

VICTIMS

Fraud attacks are increasingly targeted toward specific organizations and specific profiles of employees within

Three types of fraud

1

ACCOUNT TAKEOVER

Account takeover is when scam artists use emails to dupe accounting departments into transferring funds into illegitimate accounts.

2

VENDOR IMPERSONATION

Fraudsters send fake emails to companies asking for payment. Be vigilant and verify the authenticity of such requests before making any payments.

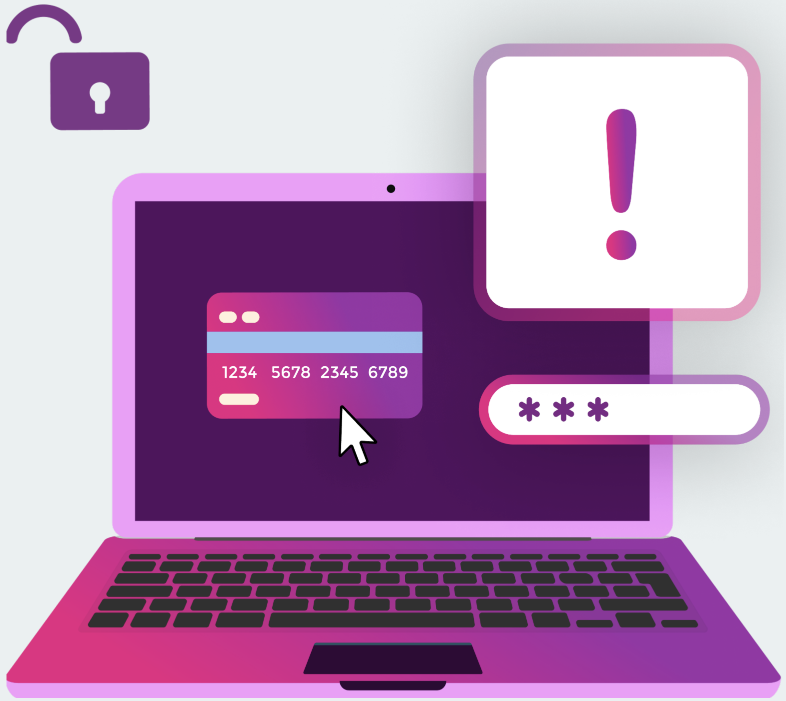
3

PHISHING

Fraudsters send a fake message designed to trick a human victim into revealing sensitive information so the attacker can expose the victim's device to malicious software.

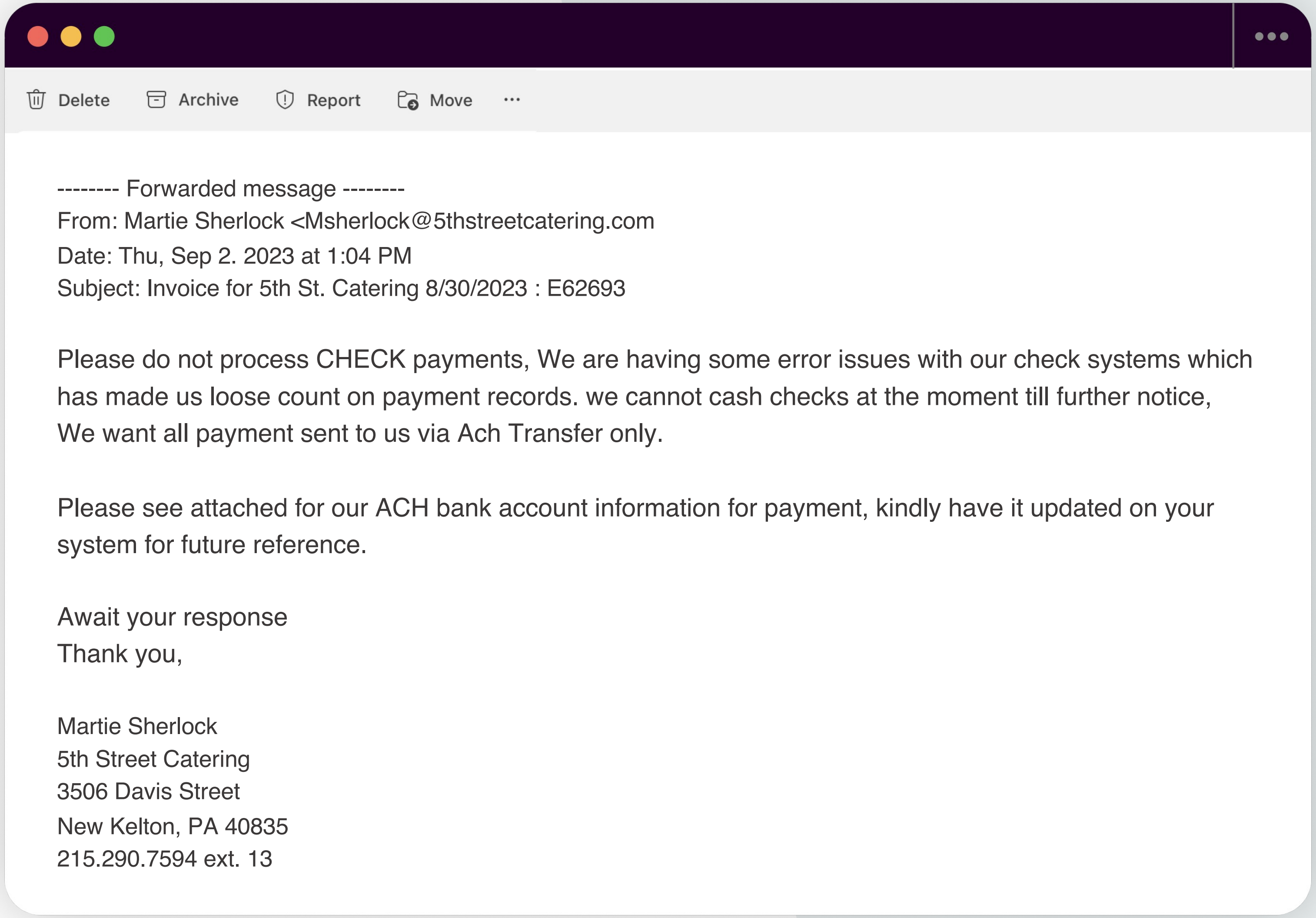
What is Account Takeover?

Scam artists use emails to dupe accounting departments into transferring funds to illegitimate accounts. Fraudsters spoof URLs and send emails pretending to be vendors or company senior management requesting either a change in bank account information or a transfer of funds to a fraudulent account.



Fraud example

ACCOUNT TAKEOVER EXAMPLE



-------- Forwarded message --------
From: Martie Sherlock <Msherlock@5thstreetcatering.com
Date: Thu, Sep 2. 2023 at 1:04 PM
Subject: Invoice for 5th St. Catering 8/30/2023 : E62693

Please do not process CHECK payments, We are having some error issues with our check systems which has made us loose count on payment records. we cannot cash checks at the moment till further notice, We want all payment sent to us via Ach Transfer only.

Please see attached for our ACH bank account information for payment, kindly have it updated on your system for future reference.

Await your response
Thank you,

Martie Sherlock
5th Street Catering
3506 Davis Street
New Kelton, PA 40835
215.290.7594 ext. 13

BEC statistics

28% OF PRACTITIONERS

INDICATE BEC THE PRIMARY SOURCE OF FRAUD ATTACKS AT THEIR ORGANIZATION

2024 AFP Payments Fraud and Control Report

47% OF ORGANIZATIONS

REPORT FRAUDSTERS ACCESSED ACH CREDITS USING BEC IN 2023

38% OF COMPANIES

EXPERIENCED FINANCIAL LOSS DUE TO FBI-REPORTED $2.9 BILLION IN BEC SCAMS

63% OF ORGANIZATIONS

WERE TARGETED BY BEC IN 2023

2024 AFP Payments Fraud and Control Report

What is Vendor Impersonation?

Fraudsters send fake emails to companies asking for payment

Sign of a fraudster

A FRAUDSTER

MIGHT USE JOHN.KELLY@COMPONY.COM (AN EXTRA “O” IN COMPANY) INSTEAD OF JOHN.KELLY@COMPANY.COM TO TRICK VICTIMS INTO THINKING THEIR EMAIL IS LEGITIMATE

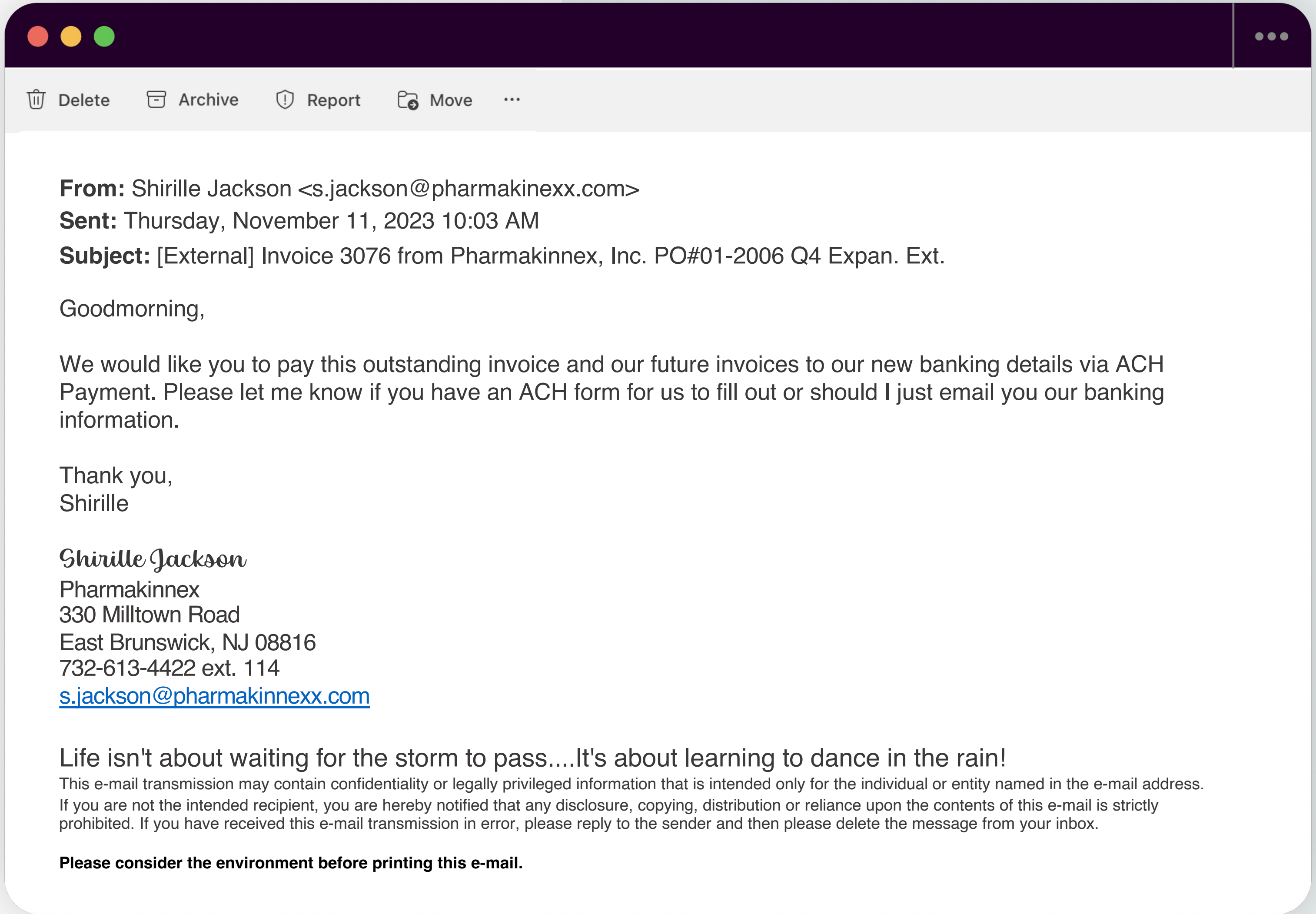
Sign of a fraudster

A FRAUDSTER

MIGHT USE jane.doe@payrnerang.com (USING AN “R” AND “N” AS AN “M”) INSTEAD OF jane.doe@paymerang.com TO TRICK VICTIMS INTO THINKING THEIR EMAIL IS LEGITIMATE

Fraud example

VENDOR IMPERSONATOR EXAMPLE



From: Shirille Jackson <s.jackson@pharmakinexx.com>
Sent: Thursday, November 11, 2023 10:03 AM
Subject: [External] Invoice 3076 from Pharmakinnex, Inc. PO#01-2006 Q4 Expan. Ext.

Goodmorning,

We would like you to pay this outstanding invoice and our future invoices to our new banking details via ACH Payment. Please let me know if you have an ACH form for us to fill out or should I just email you our banking information.

Thank you,
Shirille

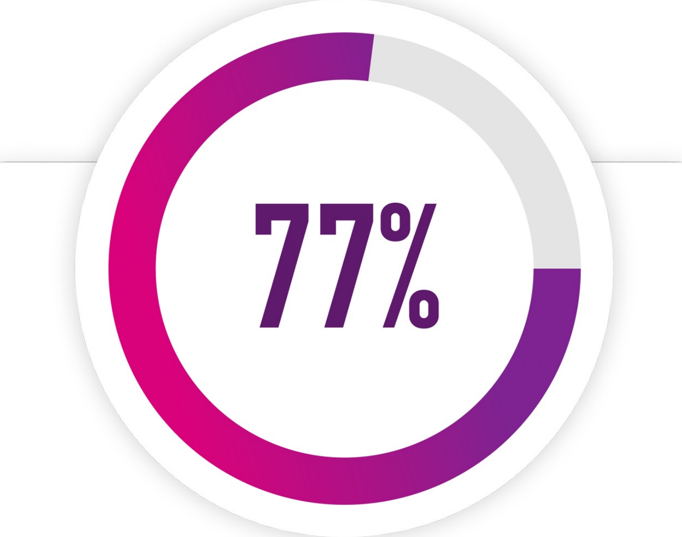
Shirille Jackson
Pharmakinnex
330 Milltown Road
East Brunswick, NJ 08816
732-613-4422 ext. 114
s.jackson@pharmakinnexx.com

Life isn't about waiting for the storm to pass....It's about learning to dance in the rain!
This e-mail transmission may contain confidentiality or legally privileged information that is intended only for the individual or entity named in the e-mail address. If you are not the intended recipient, you are hereby notified that any disclosure, copying, distribution or reliance upon the contents of this e-mail is strictly prohibited. If you have received this e-mail transmission in error, please reply to the sender and then please delete the message from your inbox.

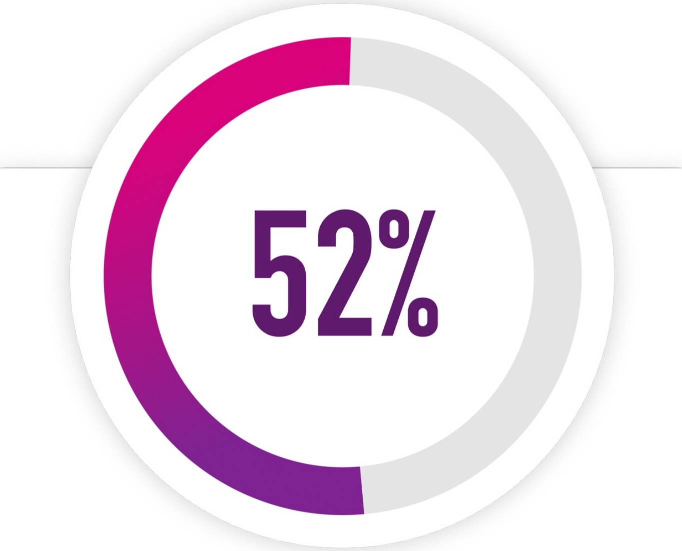
Please consider the environment before printing this e-mail.

Most prevalent types of BEC fraud in 2022

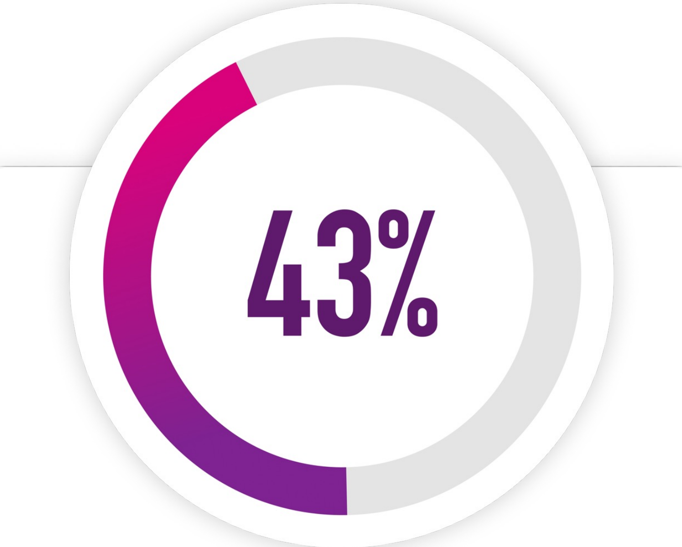
(Percent of Organizations)



SPOOF
EMAIL



DOMAIN
LOOKALIKE



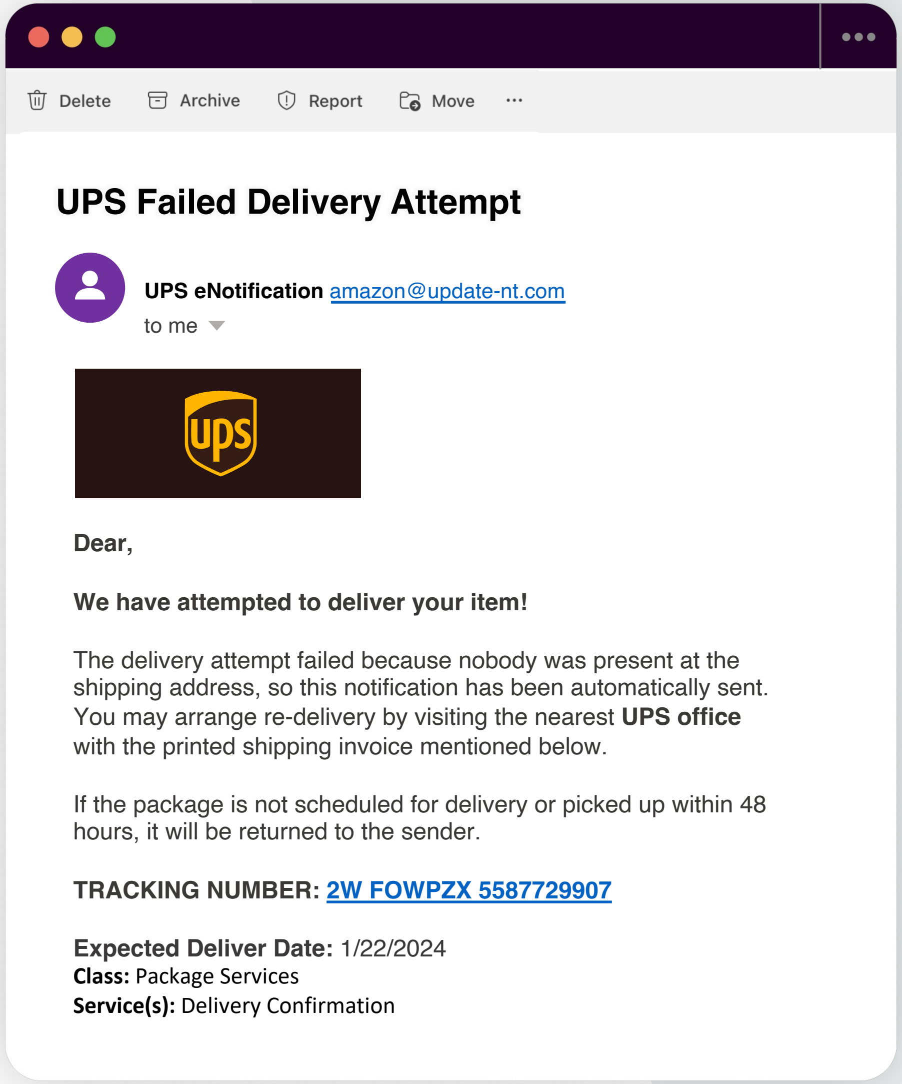
HIJACKED
EMAIL

What is Phishing?

Fraudsters send a fake message designed to trick a victim into revealing sensitive information so the attacker can expose the victim's device to malicious software, get their credit card information and passwords.

Fraud example

PHISHING EXAMPLES



UPS Failed Delivery Attempt

UPS eNotification amazon@update-nt.com

to me

Dear,

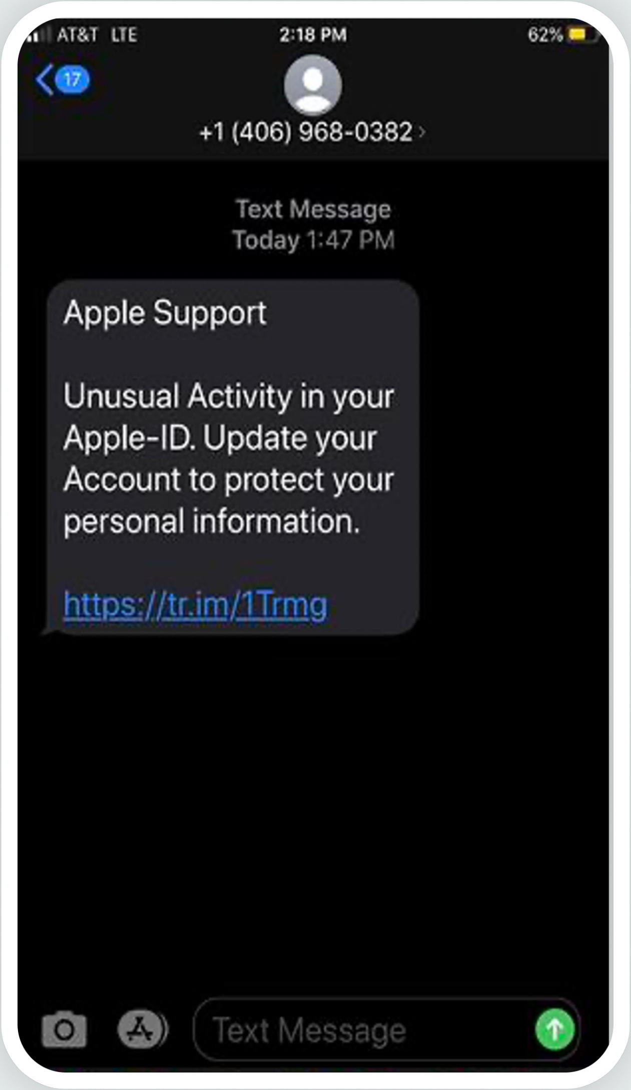
We have attempted to deliver your item!

The delivery attempt failed because nobody was present at the shipping address, so this notification has been automatically sent. You may arrange re-delivery by visiting the nearest **UPS office** with the printed shipping invoice mentioned below.

If the package is not scheduled for delivery or picked up within 48 hours, it will be returned to the sender.

TRACKING NUMBER: 2W FOWPZX 5587729907

Expected Deliver Date: 1/22/2024
Class: Package Services
Service(s): Delivery Confirmation



Text Message
Today 1:47 PM

Apple Support

Unusual Activity in your Apple-ID. Update your Account to protect your personal information.

https://tr.im/1Trmg

Practical steps

AS LONG AS THERE IS MONEY AND VALUABLE DATA, THERE WILL BE FRAUD ATTEMPTS AND THREATS TO SECURITY

PAYMENT

- Positive pay
- Use one-time use, preloaded virtual cards
- Encrypt account information
- Verify vendors before making changes
- Limit employee access
- Require approval for changes

OPERATIONS

- Clean desk and secure documents
- Utilize certified shredding service
- Verify anomalous changes
- Assign fraud scores
- Suspicious links and fraudulent email detection training
- Multiple approvals
- Single payment limits
- Segregation of duties
- Job rotation and cross training
- Defined access controls

COMPLIANCE

- NACHA – read it, learn it, train it
- Do not store banking data if you can avoid it
- PCI – Secure cardholder data
- SOC 2 – Security controls for integrity and confidentiality
- OFAC – Know your vendor and where your money is going

What is Ransomware?

The difference between ransomware and malware is that not all ransomware involves data being encrypted.

Ransomware statistics

Every 11 seconds
an organization falls victim
to a **ransomware attack**

Source: Astra 100+ Ransomware Attack Statistics 2024: Trends & Cost Article

In the past 5 years
there has been a **13% increase**
in **ransomware attacks**

Source: Astra 100+ Ransomware Attack Statistics 2024: Trends & Cost Article

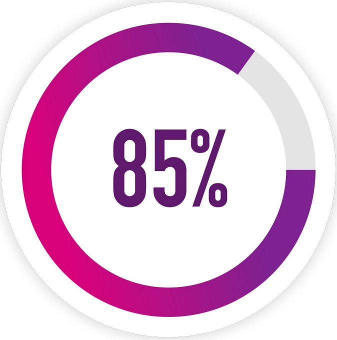
It costs $1.85 million
on average **to recover** from
an **attack** in 2023

Source: Astra 100+ Ransomware Attack Statistics 2024: Trends & Cost Article

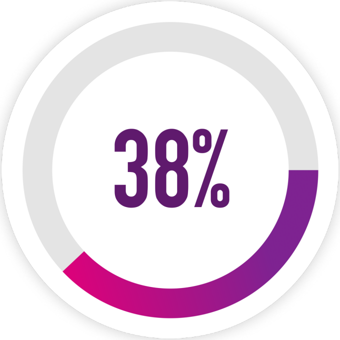
18 days
is the average **downtime**

Source: Statista Cyber Crime & Security Survey 2023

Ransomware statistics

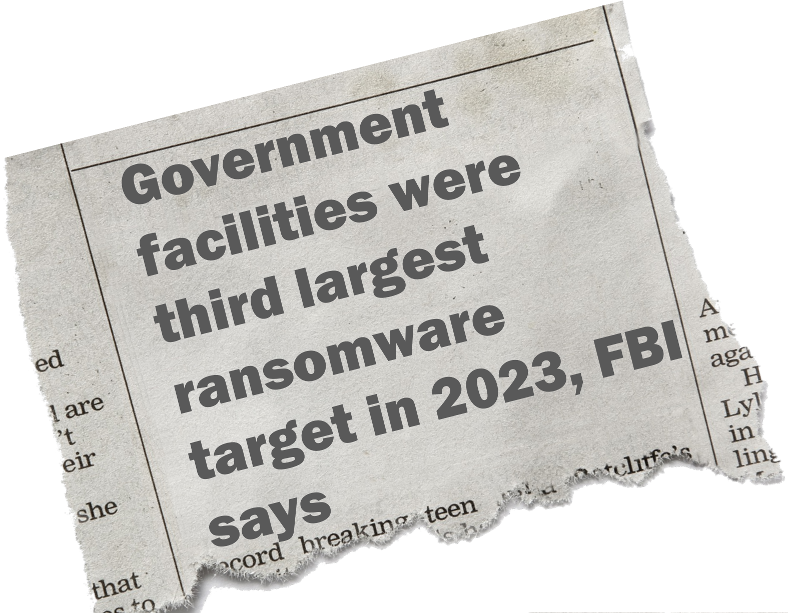


85% of businesses think their organization is at least somewhat prepared for a ransomware attack.

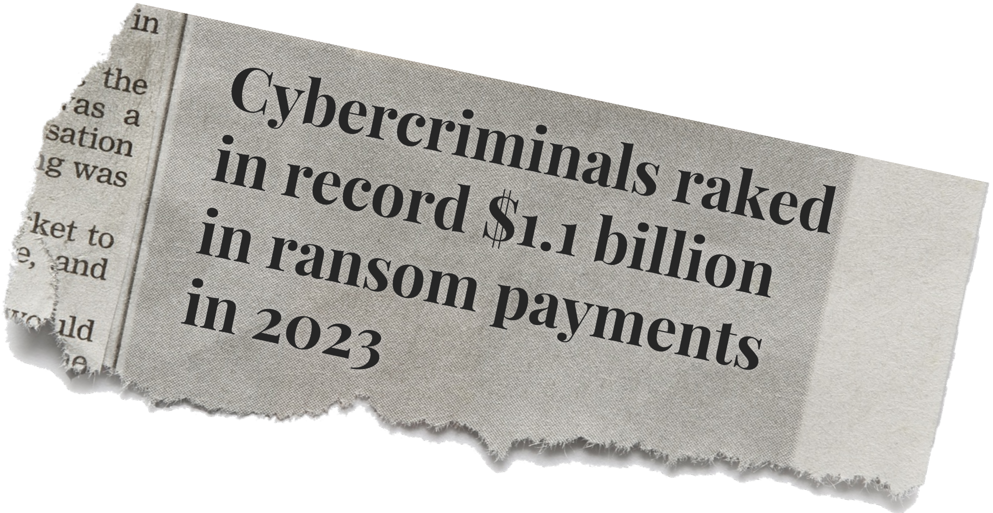


38% of businesses think their organization is at least somewhat prepared for a ransomware attack.

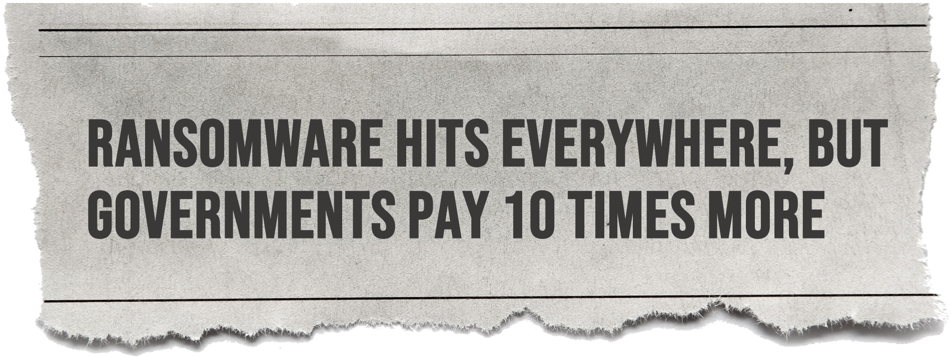
Fraud in the news



Government facilities were third largest ransomware target in 2023, FBI says



Cybercriminals raked in record $1.1 billion in ransom payments in 2023



RANSOMWARE HITS EVERYWHERE, BUT GOVERNMENTS PAY 10 TIMES MORE

Why victims pay

92%

92 PERCENT WHO PAY THE RANSOM, DON'T GET THEIR DATA BACK

Paying a ransom doesn't guarantee that the hacker will unencrypt of unlock the stolen/locked data

Why do victims pay?

- Lack of data back up
- Desperation
- Want data decrypted

Practical steps

AS LONG AS THERE IS MONEY AND VALUABLE DATA, THERE WILL BE FRAUD ATTEMPTS AND THREATS TO SECURITY

NETWORK

- Antivirus Software and whitelisting technology
- Vulnerability management program
- Security posture scanning
- Software patching
- Expert penetration testing
- Spam and phishing defenses
- Email encryption
- Multi-factor authentication

Scan QR code or visit www.paymerang.com

MICHAEL DOERR

mdoerr@paymerang.com | 804-575-5646