DiscoverSeneca
Seneca County Chamber of Commerce

CYBERSECURITY 2023

EDUCATIONAL WEBINAR

McMANUS IT
SOLUTIONS

AGENDA

- INTRODUCTION
- STATE OF CYBERSECURITY 2023
- PHISHING
- SOCIAL MEDIA
- WHAT IS RANSOMWARE?
- WHY YOU SHOULD CARE
- STEPS TO PROTECT
- Q&A + CLOSING

INTRODUCTION

STATE OF CYBERSECURITY 2023

- Cybersecurity threats are increasing exponentially
- Over half of SMB have reported being the victims of cybercrimes
- The average cost of a data breach for SMB is $149,000 in 2021
- Ransomware has evolved to be more sophisticated and efficient, targeting local backups
- Malicious actors are getting better at evading detection by standard cloud security measures and protocols

SOCIAL MEDIA

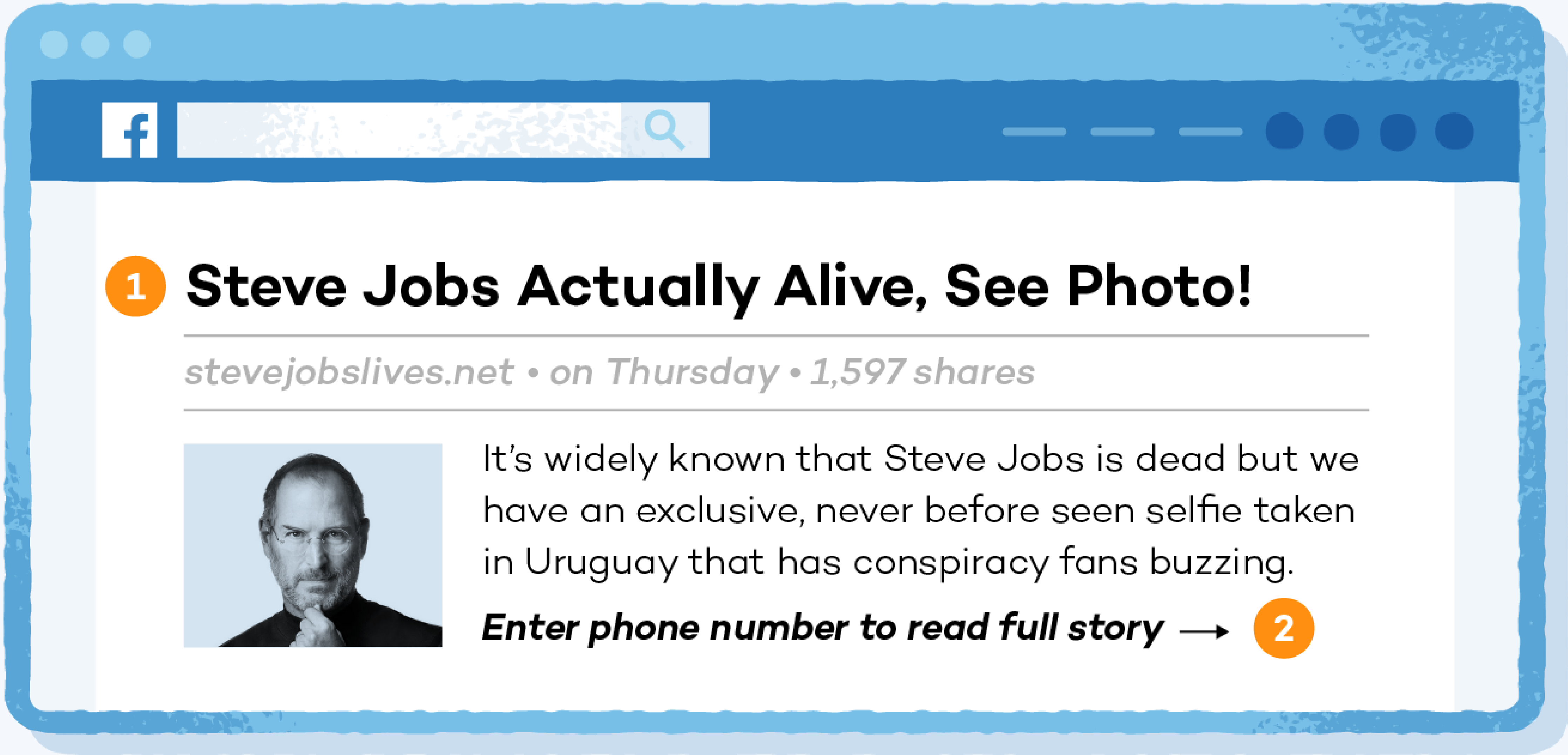
SCAMS TO WATCH FOR

SOCIAL MEDIA: KEY INDICATORS

URGENT

FAMILIAR

CALL TO ACTION



1 **Steve Jobs Actually Alive, See Photo!**

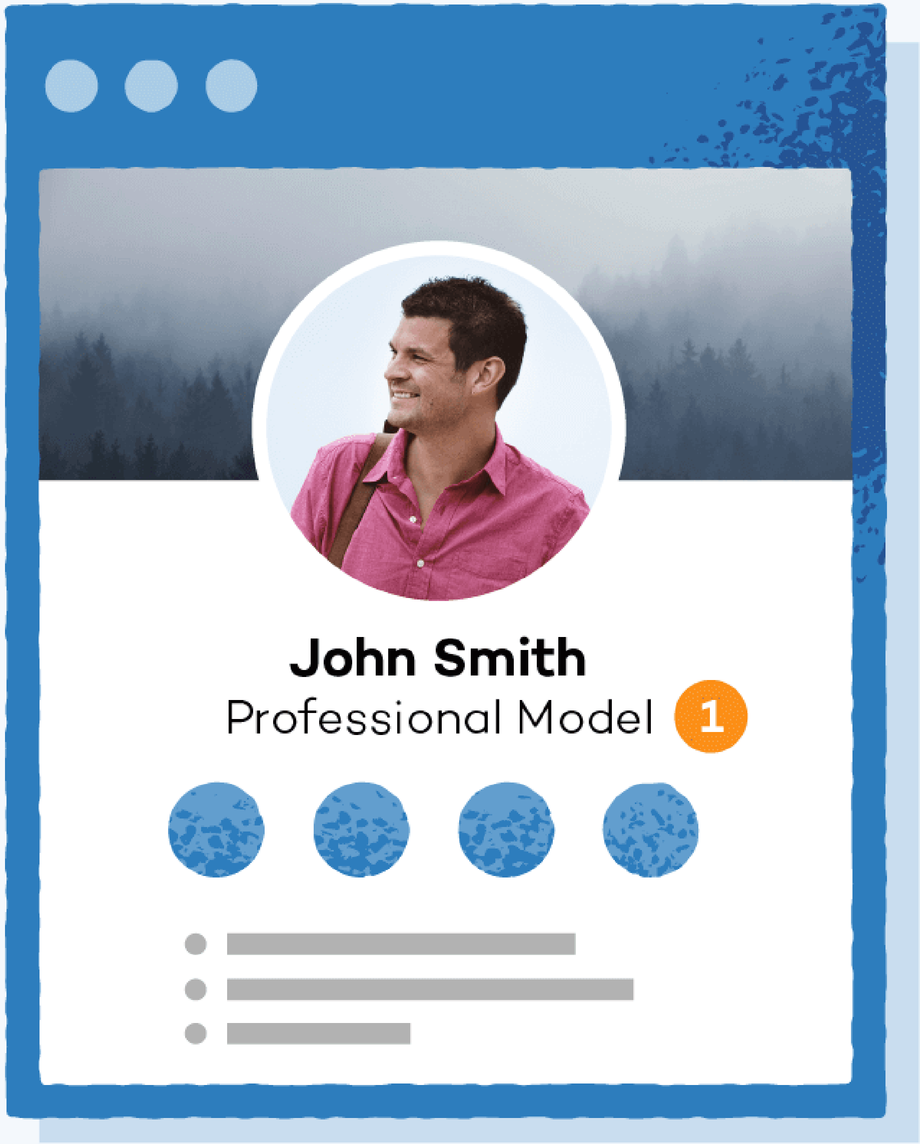
stevejobslives.net • on Thursday • 1,597 shares

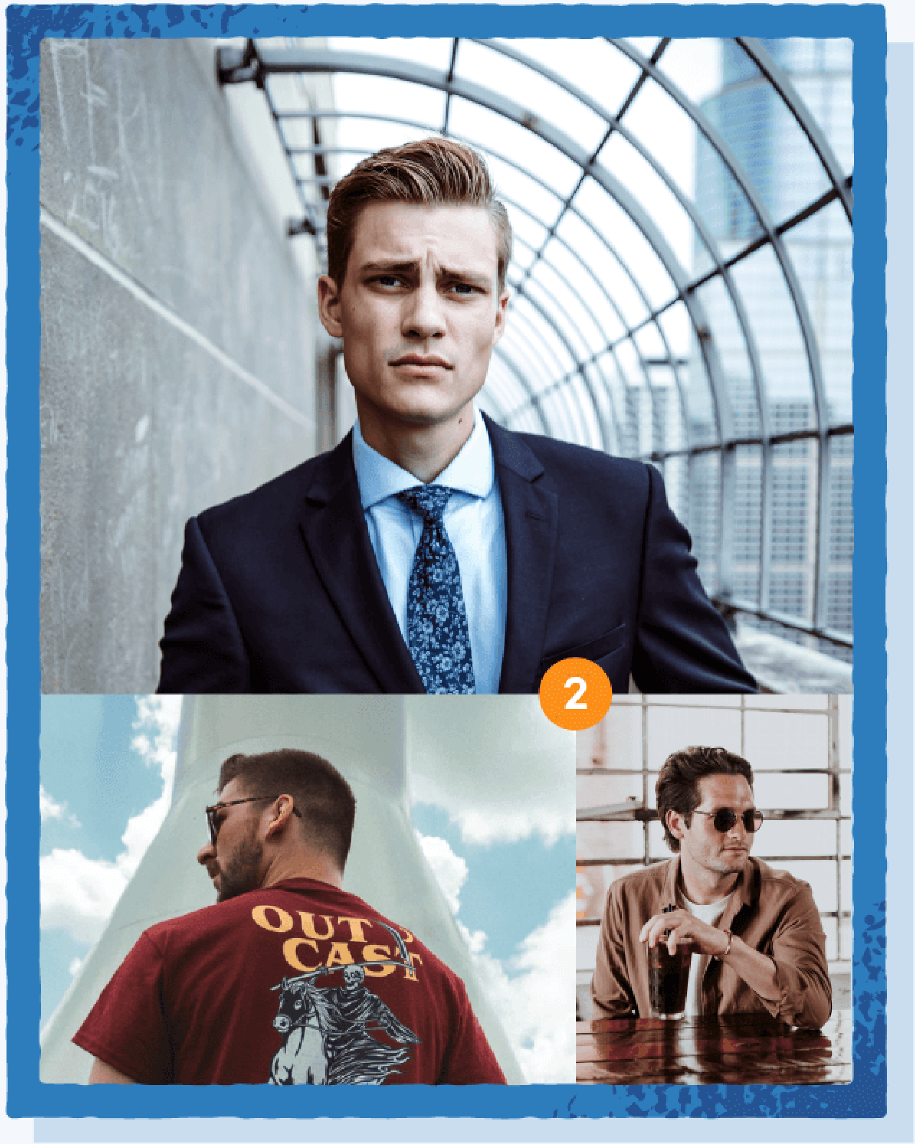
It’s widely known that Steve Jobs is dead but we have an exclusive, never before seen selfie taken in Uruguay that has conspiracy fans buzzing.

Enter phone number to read full story → 2

1 Gossip headline

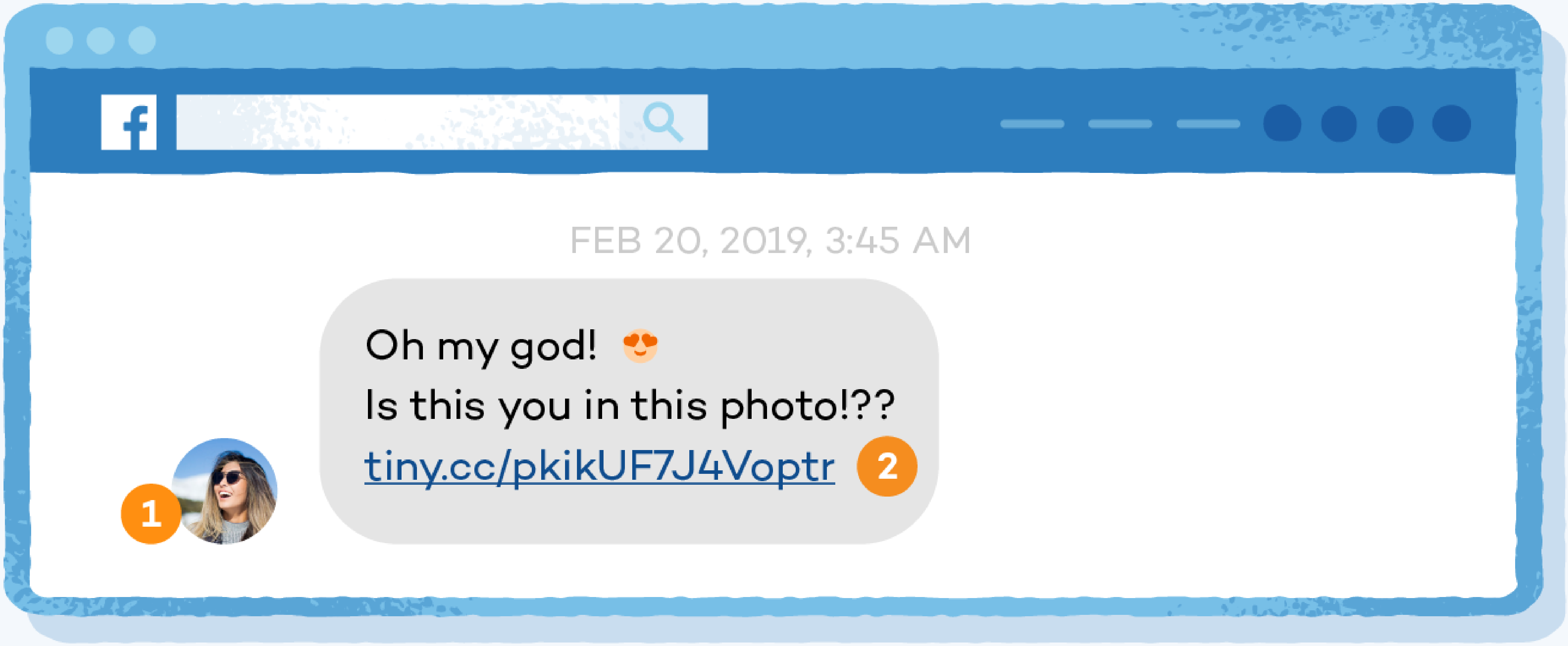
2 Requests personal information





1 Glamorous profession

2 Inconsistencies in photos and facts

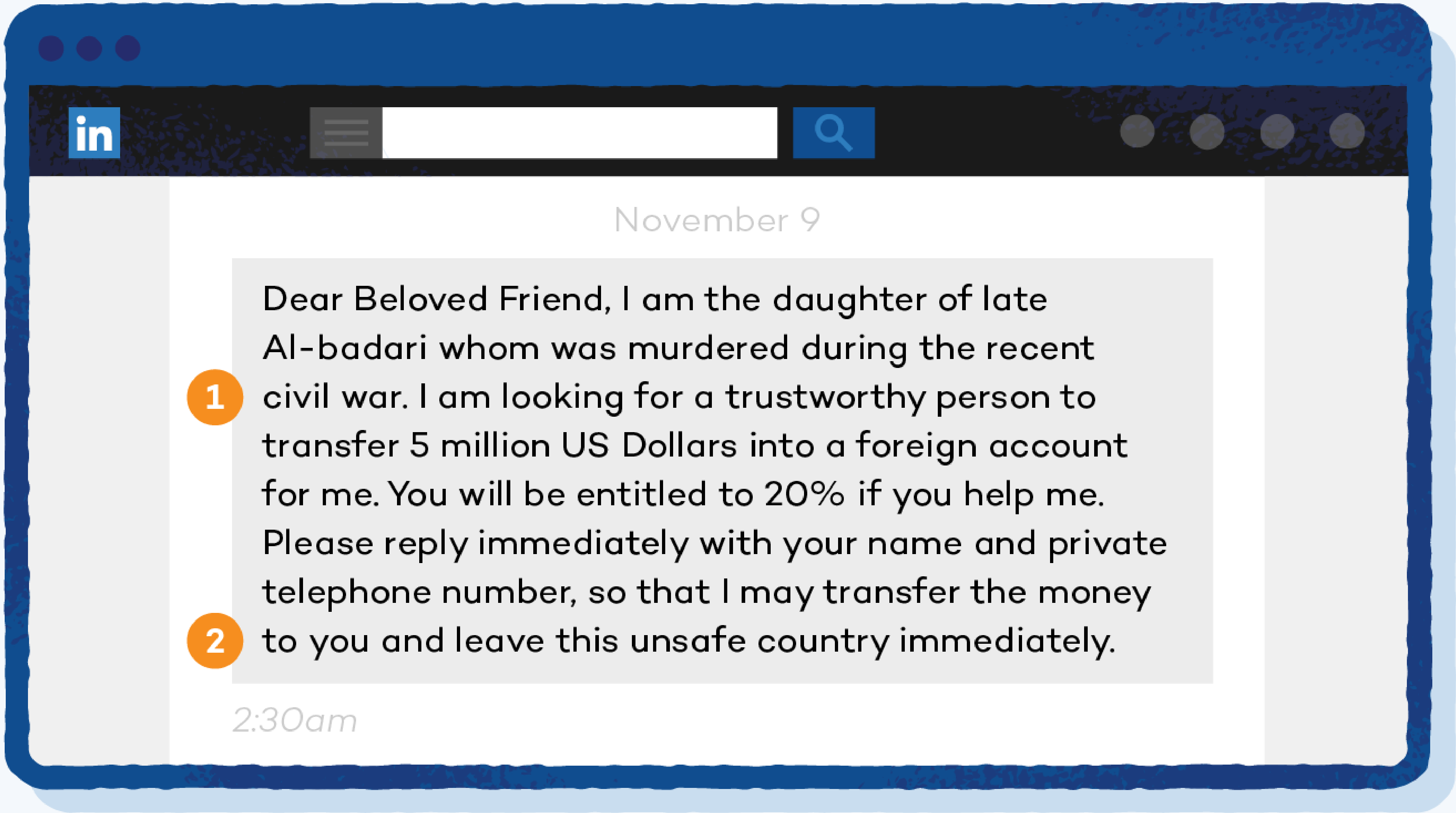


FEB 20, 2019, 3:45 AM

Oh my god! 😍
Is this you in this photo!??
tiny.cc/pkikUF7J4Voptr

1 Unfamiliar contact photo

2 Sketchy link



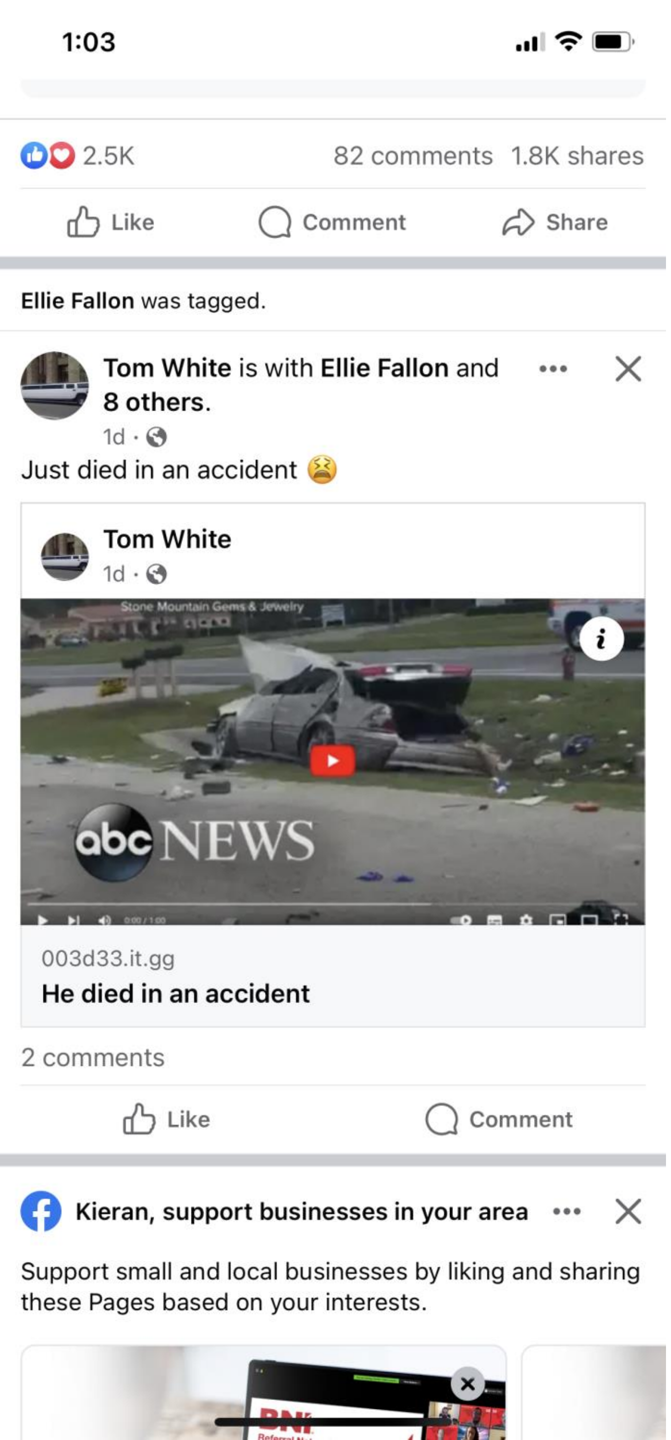
November 9

Dear Beloved Friend, I am the daughter of late Al-badari whom was murdered during the recent civil war. I am looking for a trustworthy person to transfer 5 million US Dollars into a foreign account for me. You will be entitled to 20% if you help me. Please reply immediately with your name and private telephone number, so that I may transfer the money to you and leave this unsafe country immediately.

2:30am

1 A tragedy scenario

2 Urgent call to action



Ellie Fallon was tagged.

Tom White is with **Ellie Fallon** and **8 others**.

1d ·

Just died in an accident 😫

Tom White

1d ·

003d33.it.gg

He died in an accident

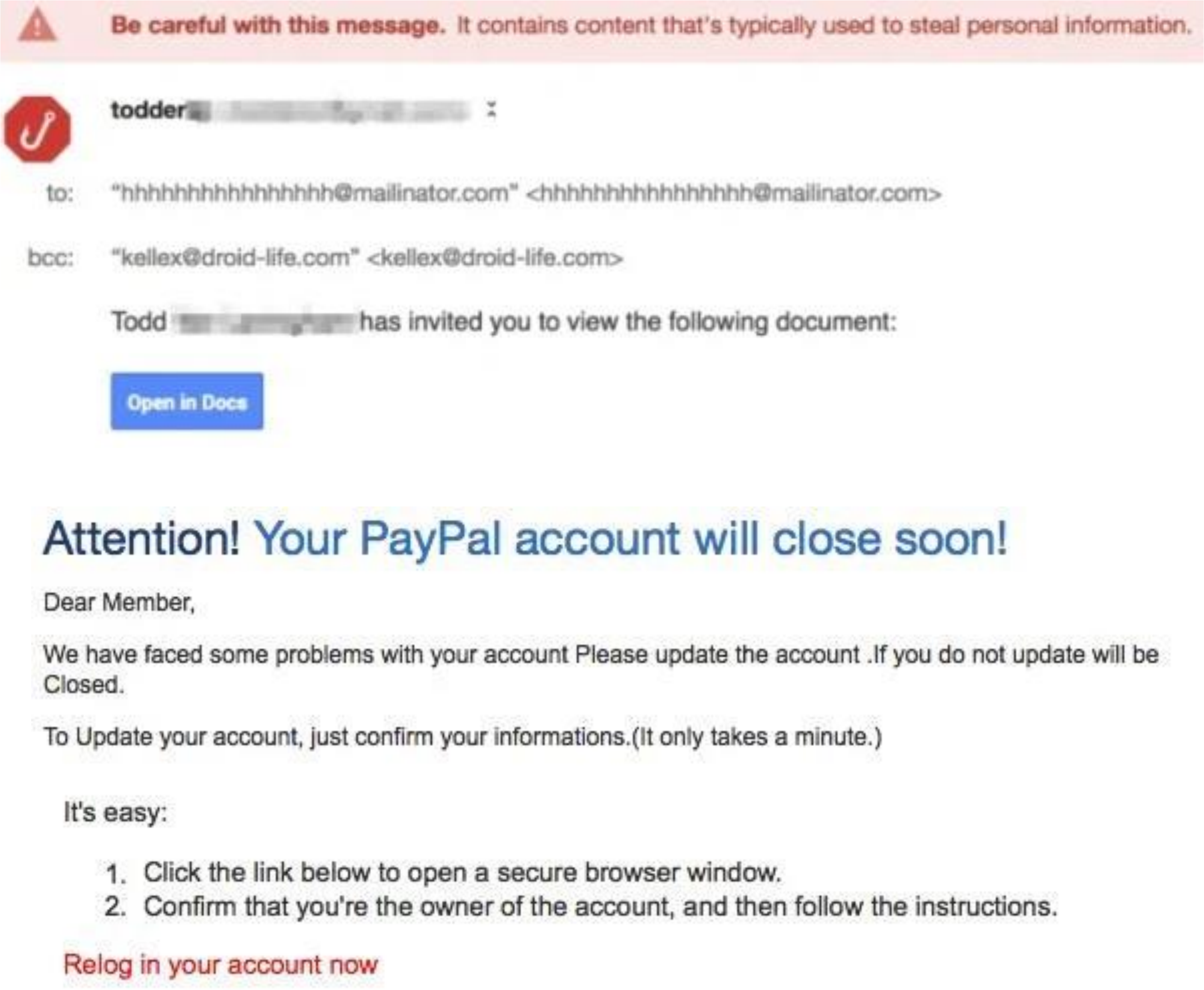
2 comments

Kieran, support businesses in your area

Support small and local businesses by liking and sharing these Pages based on your interests.

PHISHING

LET'S DIVE IN



Be careful with this message. It contains content that's typically used to steal personal information.

todder[redacted]

to: "hhhhhhhhhhhhhhhh@mailinator.com" <hhhhhhhhhhhhhhhh@mailinator.com>

bcc: "kellex@droid-life.com" <kellex@droid-life.com>

Todd [redacted] has invited you to view the following document:

Attention! Your PayPal account will close soon!

Dear Member,

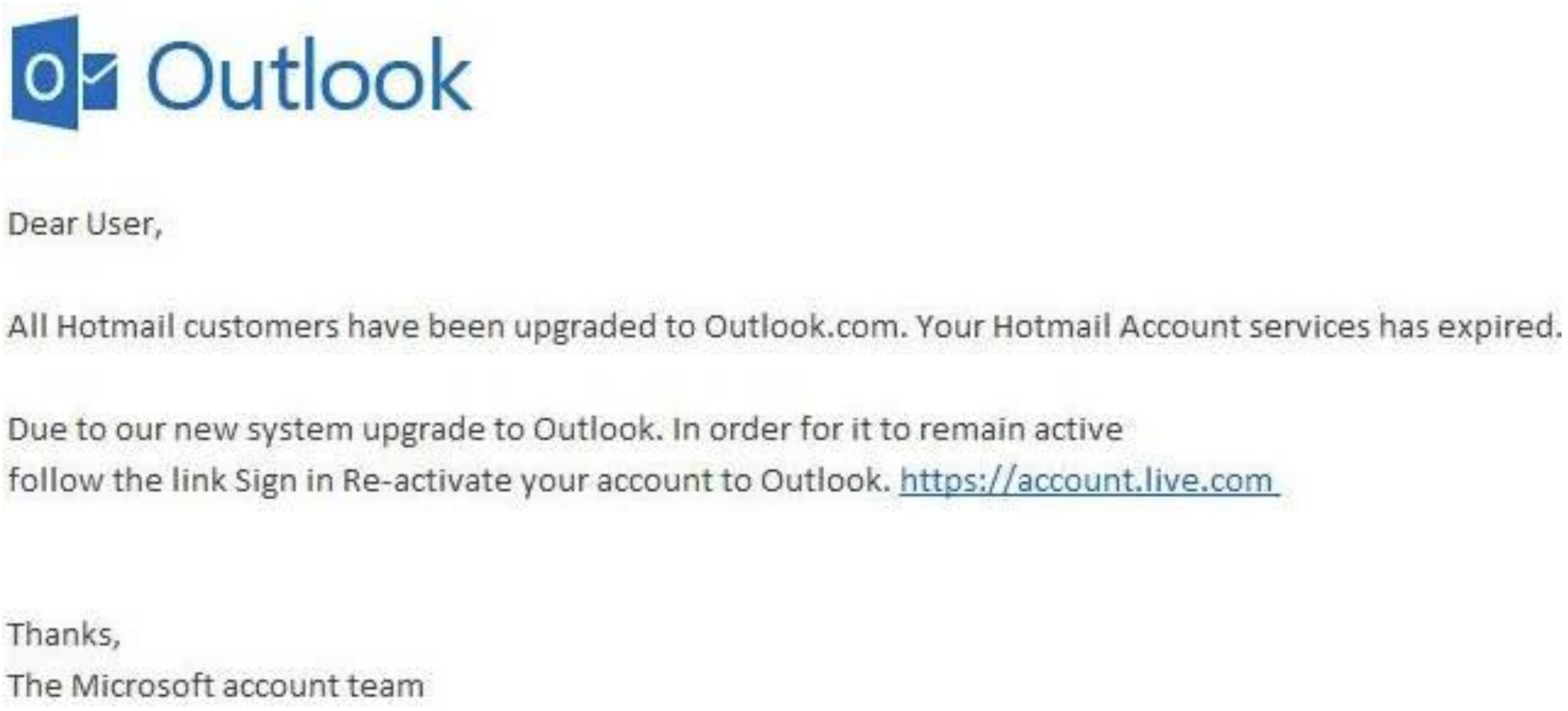
We have faced some problems with your account Please update the account .If you do not update will be Closed.

To Update your account, just confirm your informations.(It only takes a minute.)

It's easy:

1. Click the link below to open a secure browser window.
2. Confirm that you're the owner of the account, and then follow the instructions.

Relog in your account now



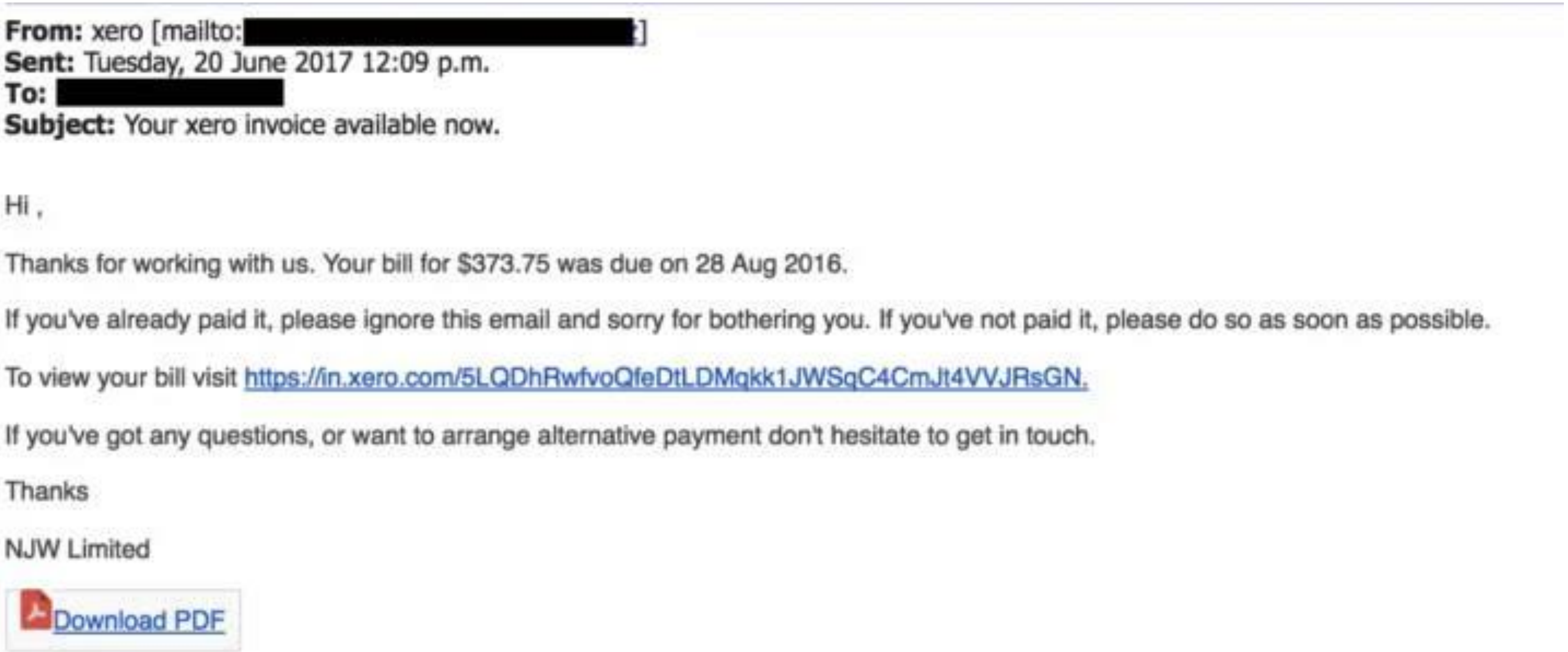
Outlook

Dear User,

All Hotmail customers have been upgraded to Outlook.com. Your Hotmail Account services has expired.

Due to our new system upgrade to Outlook. In order for it to remain active
follow the link Sign in Re-activate your account to Outlook. https://account.live.com

Thanks,
The Microsoft account team



From: xero [mailto:[redacted]]
Sent: Tuesday, 20 June 2017 12:09 p.m.
To: [redacted]
Subject: Your xero invoice available now.

Hi ,

Thanks for working with us. Your bill for $373.75 was due on 28 Aug 2016.

If you've already paid it, please ignore this email and sorry for bothering you. If you've not paid it, please do so as soon as possible.

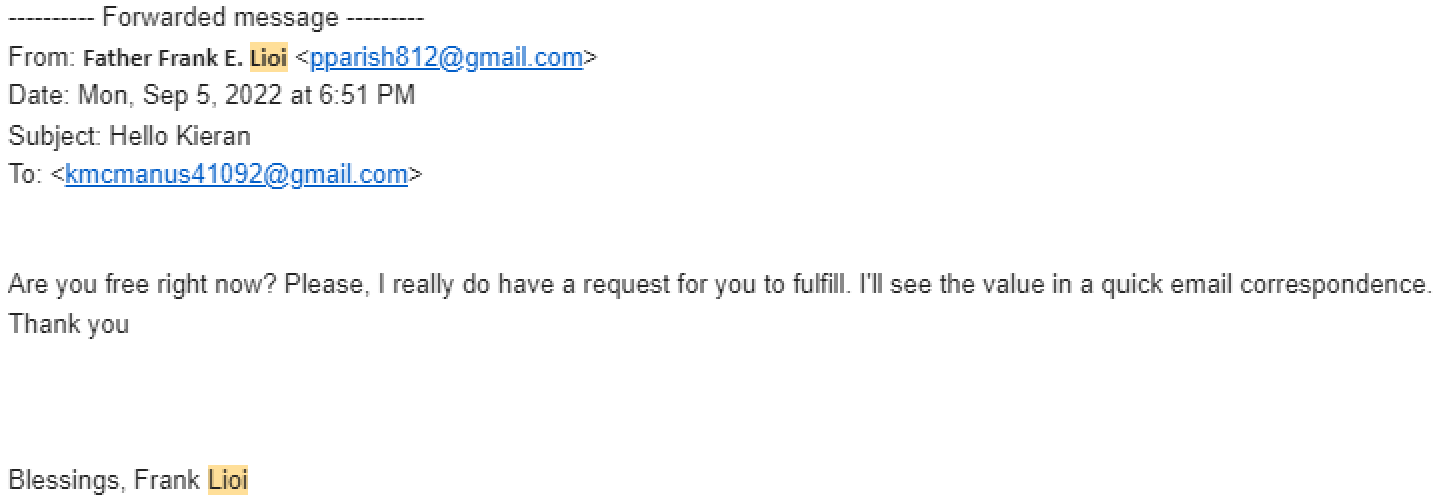
To view your bill visit https://in.xero.com/5LQDhRwfvoQfeDtLDMqkk1JWSqC4CmJt4VVJRsGN.

If you've got any questions, or want to arrange alternative payment don't hesitate to get in touch.

Thanks

NJW Limited

SPEAR PHISHING



---------- Forwarded message ---------
From: **Father Frank E. Lioi** <pparish812@gmail.com>
Date: Mon, Sep 5, 2022 at 6:51 PM
Subject: Hello Kieran
To: <kmcmanus41092@gmail.com>

Are you free right now? Please, I really do have a request for you to fulfill. I'll see the value in a quick email correspondence.
Thank you

Blessings, Frank Lioi

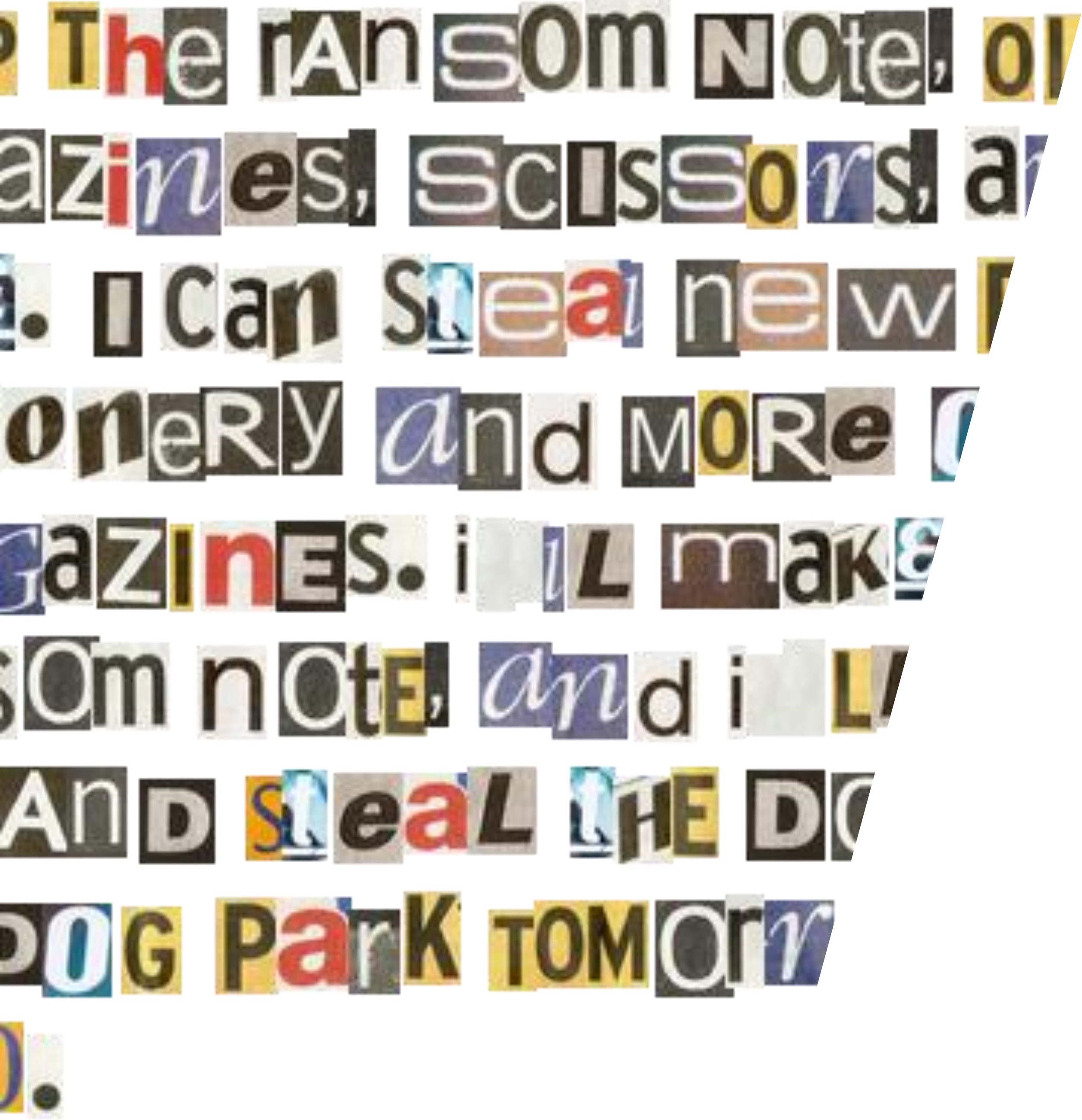
PHISHING: KEY INDICATORS

URGENT

FAMILIAR/

TRUSTED DOMAIN

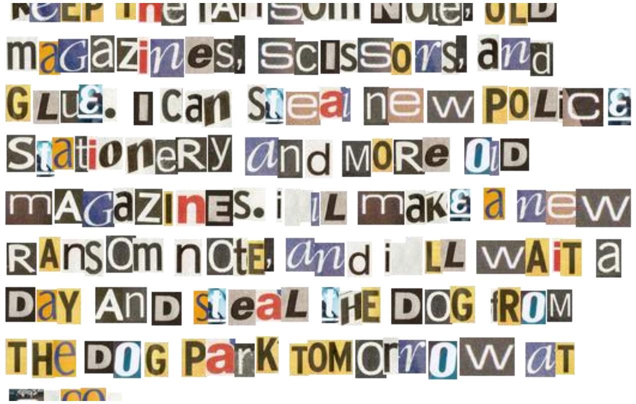
CALL TO ACTION



WHAT IS RANSOMWARE?

LET'S DIVE IN

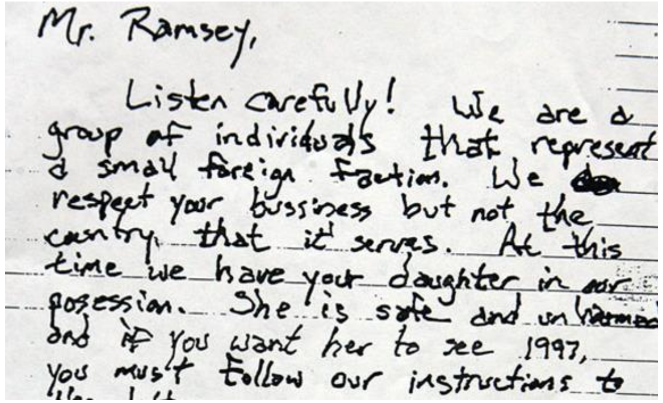
RANSOMWARE



Keep the ransom note, old magazines, scissors, and glue. I can steal new police stationery and more old magazines. i 'll make a new ransom note, and i 'll wait a day and steal the dog from the dog park tomorrow at

RANSOM NOTE:

letter demanding goods/service in exchange for something or someone being held hostage

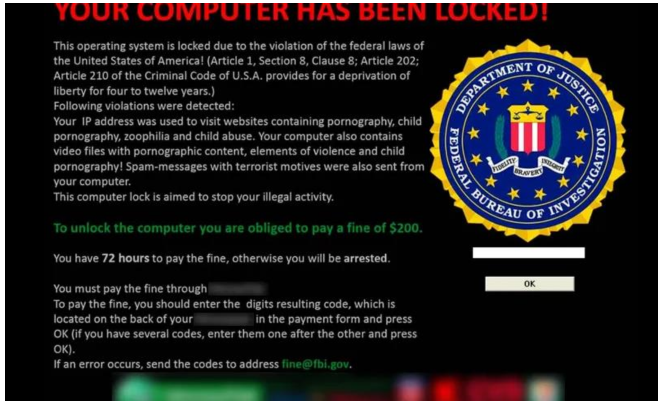


Mr. Ramsey,

Listen carefully! We are a group of individuals that represent a small foreign faction. We respect your bussiness but not the country that it serves. At this time we have your daughter in our posession. She is safe and unharmed and if you want her to see 1997, you must follow our instructions to

RANSOM:

a sum of money or other payment demanded or paid for the release of a prisoner



YOUR COMPUTER HAS BEEN LOCKED!

This operating system is locked due to the violation of the federal laws of the United States of America! (Article 1, Section 8, Clause 8; Article 202; Article 210 of the Criminal Code of U.S.A. provides for a deprivation of liberty for four to twelve years.)
Following violations were detected:
Your IP address was used to visit websites containing pornography, child pornography, zoophilia and child abuse. Your computer also contains video files with pornographic content, elements of violence and child pornography! Spam-messages with terrorist motives were also sent from your computer.
This computer lock is aimed to stop your illegal activity.

To unlock the computer you are obliged to pay a fine of $200.

You have **72 hours** to pay the fine, otherwise you will be **arrested**.

You must pay the fine through [redacted]
To pay the fine, you should enter the digits resulting code, which is located on the back of your [redacted] in the payment form and press OK (if you have several codes, enter them one after the other and press OK).
If an error occurs, send the codes to address fine@fbi.gov.

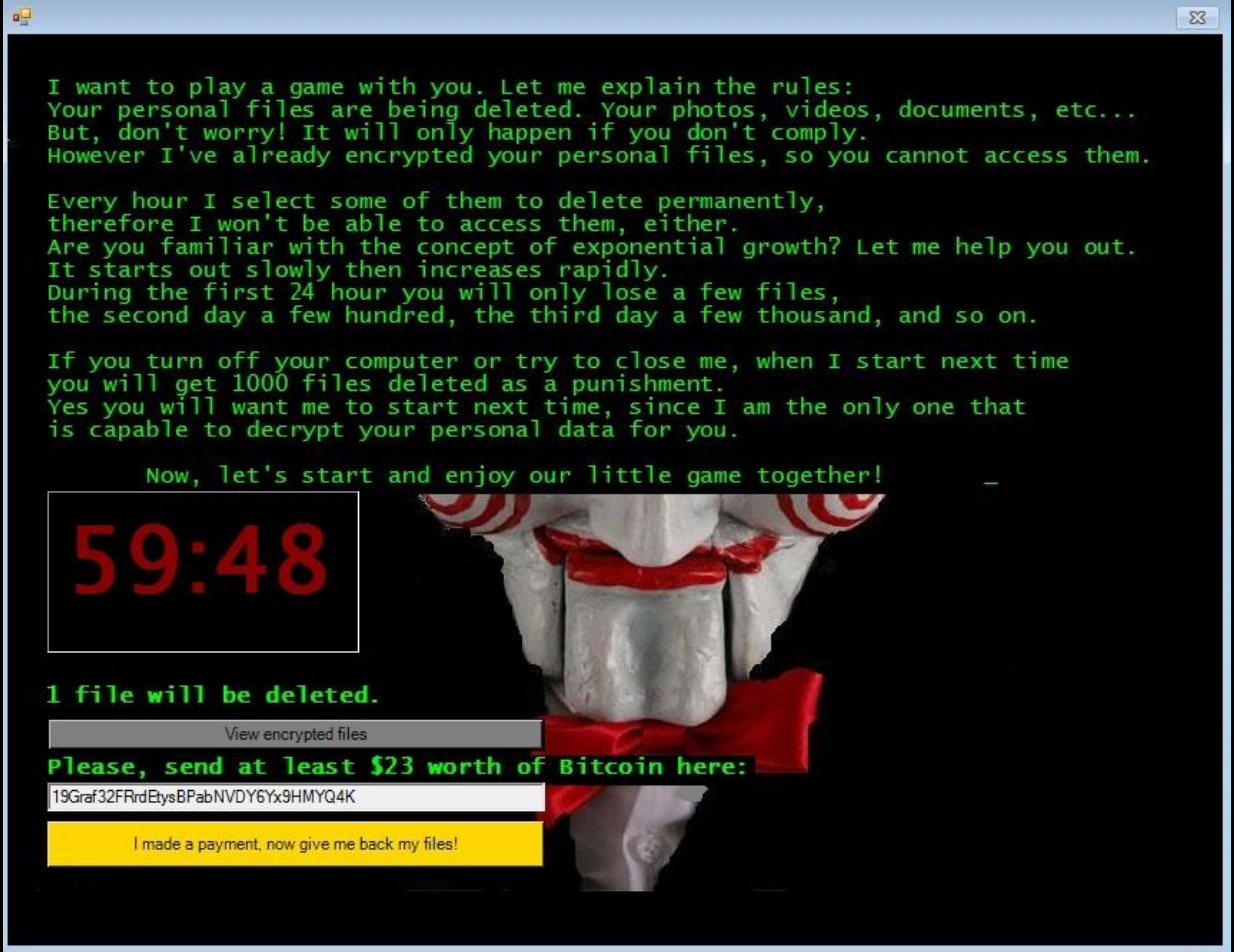
RANSOMWARE:

a type of malicious software designed to block access to a computer system until a sum of money is paid

ENCRYPTION

The process of converting information or data into a code, especially to prevent unauthorized access

Encrypted data is undecipherable without an encryption key. Good + Bad.



I want to play a game with you. Let me explain the rules:
Your personal files are being deleted. Your photos, videos, documents, etc...
But, don't worry! It will only happen if you don't comply.
However I've already encrypted your personal files, so you cannot access them.

Every hour I select some of them to delete permanently,
therefore I won't be able to access them, either.
Are you familiar with the concept of exponential growth? Let me help you out.
It starts out slowly then increases rapidly.
During the first 24 hour you will only lose a few files,
the second day a few hundred, the third day a few thousand, and so on.

If you turn off your computer or try to close me, when I start next time
you will get 1000 files deleted as a punishment.
Yes you will want me to start next time, since I am the only one that
is capable to decrypt your personal data for you.

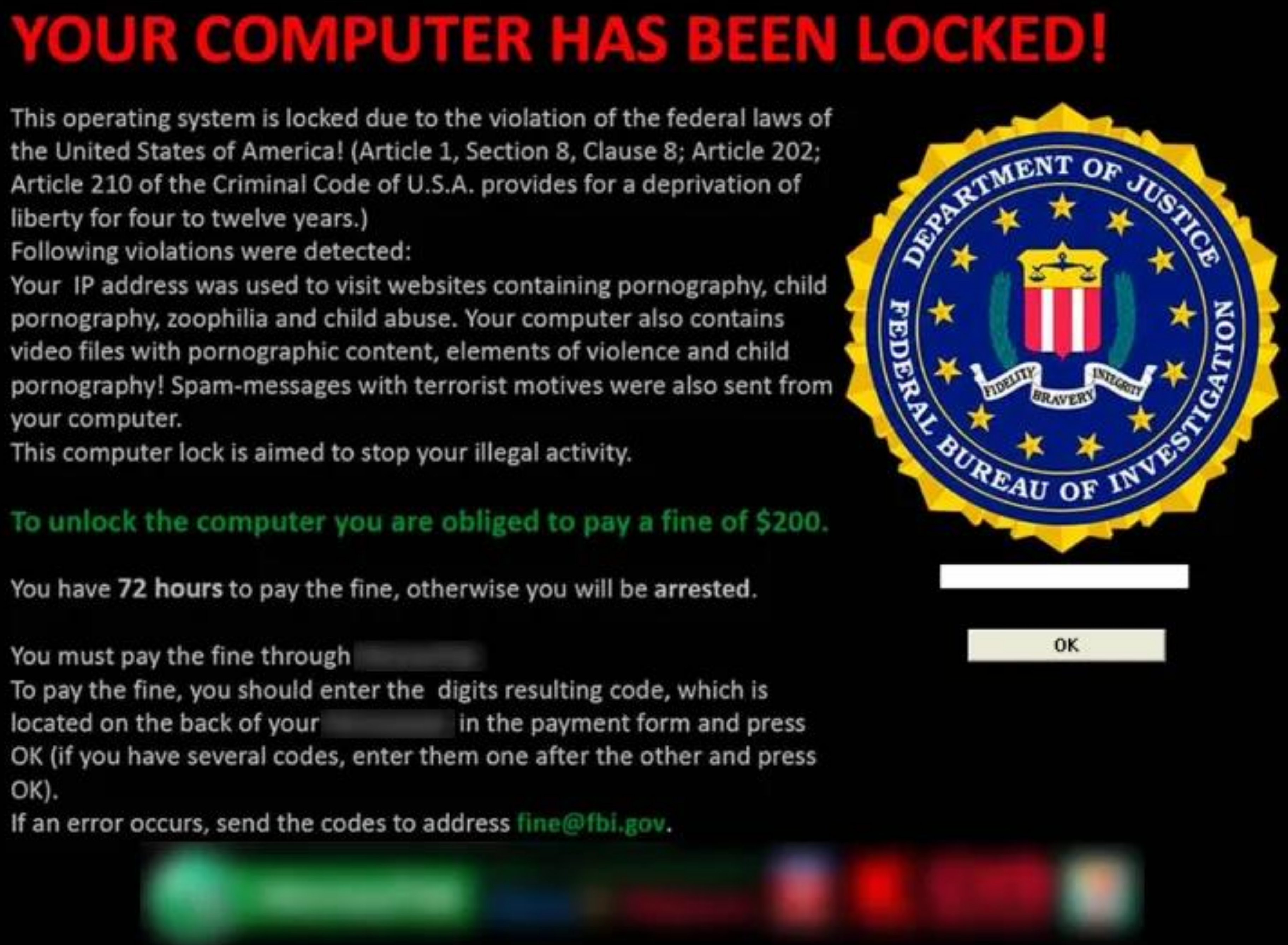
Now, let's start and enjoy our little game together!

59:48

1 file will be deleted.

Please, send at least $23 worth of Bitcoin here:

19Graf32FRrdEtysBPabNVDY6Yx9HMYQ4K



YOUR COMPUTER HAS BEEN LOCKED!

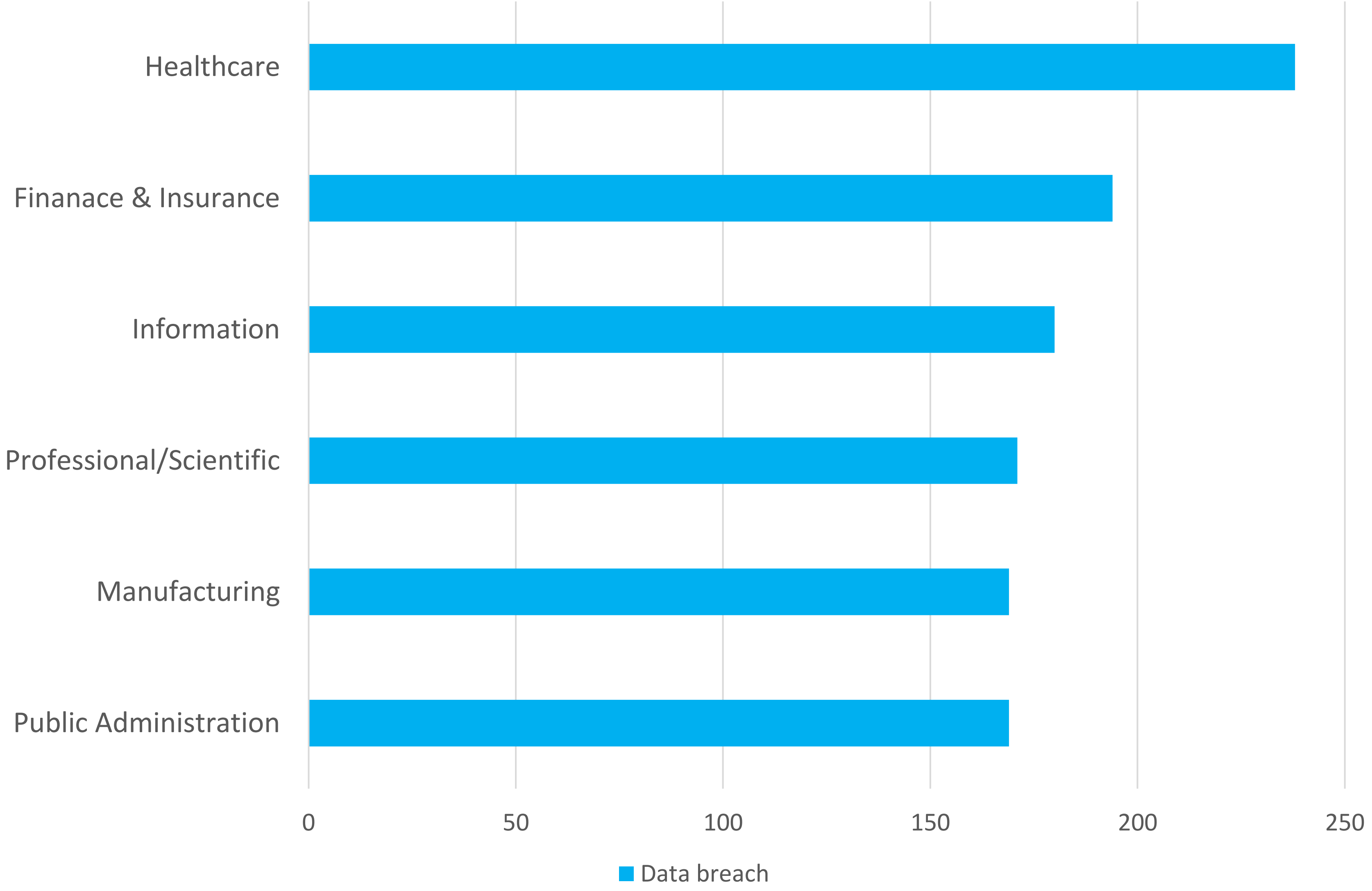
This operating system is locked due to the violation of the federal laws of the United States of America! (Article 1, Section 8, Clause 8; Article 202; Article 210 of the Criminal Code of U.S.A. provides for a deprivation of liberty for four to twelve years.)
Following violations were detected:
Your IP address was used to visit websites containing pornography, child pornography, zoophilia and child abuse. Your computer also contains video files with pornographic content, elements of violence and child pornography! Spam-messages with terrorist motives were also sent from your computer.
This computer lock is aimed to stop your illegal activity.

To unlock the computer you are obliged to pay a fine of $200.

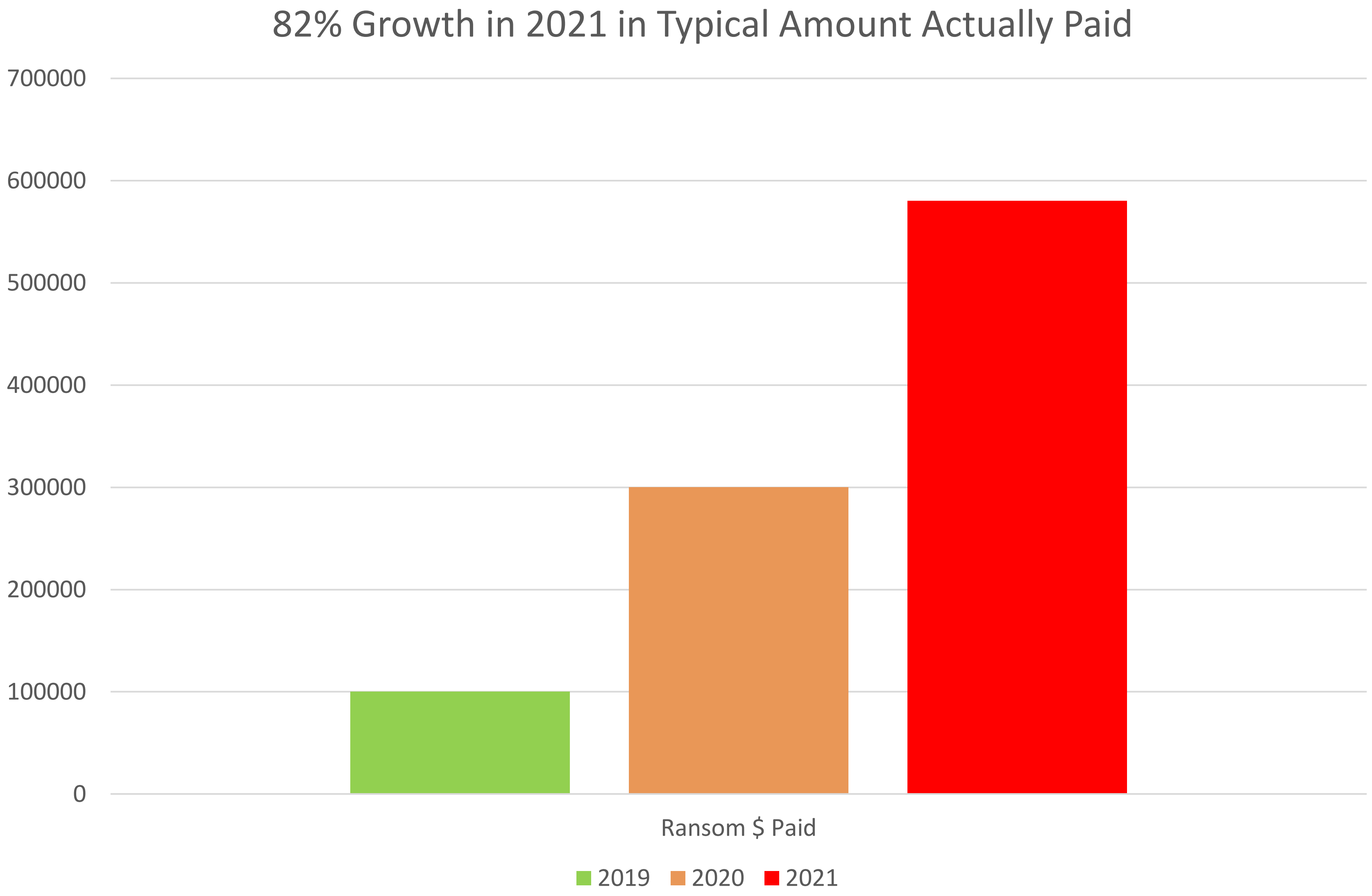
You have **72 hours** to pay the fine, otherwise you will be arrested.

You must pay the fine through [redacted]
To pay the fine, you should enter the digits resulting code, which is located on the back of your [redacted] in the payment form and press OK (if you have several codes, enter them one after the other and press OK).
If an error occurs, send the codes to address fine@fbi.gov.

WHO WAS BREACHED IN 2021?



AVERAGE RANSOM PAYMENTS



AVERAGE RANSOM PAYMENTS

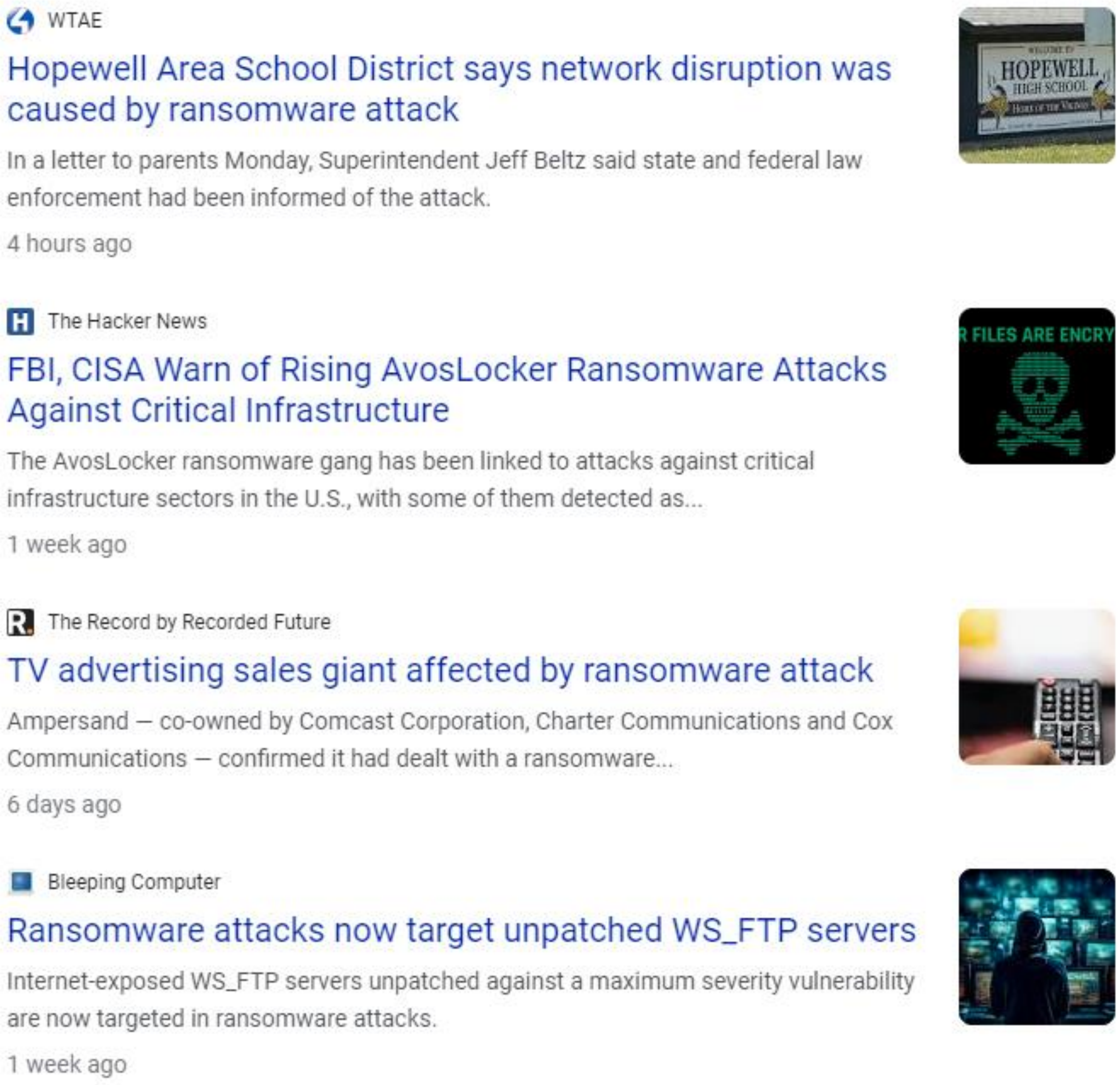
The rate of ransomware attacks has remained level, with 66% of respondents reporting that their organization was hit by ransomware in the previous year

It cost companies on average $1.82 million to recover from a ransomware attack in 2023

For companies with annual revenue of less than $10 million, the average cost of recovery was $165,520. For companies with annual revenue greater than $5 billion, the average cost of recovery approached $5 million. *(Sophos 2023 State of Ransomware)*

It is not a question of IF, but WHEN you may encounter an attack

No business is too small, just too small to make the news



WTAE

Hopewell Area School District says network disruption was caused by ransomware attack

In a letter to parents Monday, Superintendent Jeff Beltz said state and federal law enforcement had been informed of the attack.

4 hours ago

The Hacker News

FBI, CISA Warn of Rising AvosLocker Ransomware Attacks Against Critical Infrastructure

The AvosLocker ransomware gang has been linked to attacks against critical infrastructure sectors in the U.S., with some of them detected as...

1 week ago

The Record by Recorded Future

TV advertising sales giant affected by ransomware attack

Ampersand — co-owned by Comcast Corporation, Charter Communications and Cox Communications — confirmed it had dealt with a ransomware...

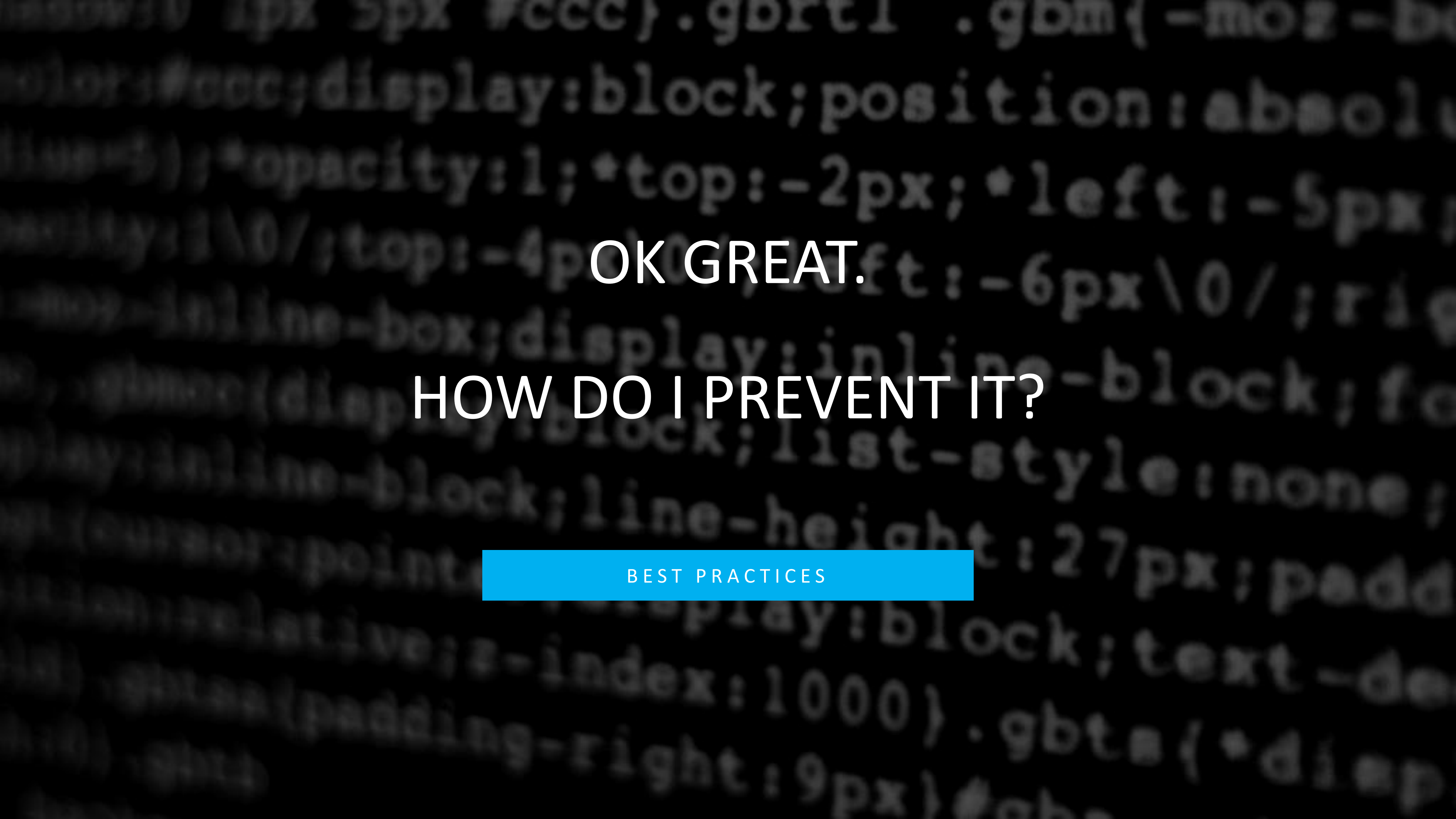
6 days ago

Bleeping Computer

Ransomware attacks now target unpatched WS_FTP servers

Internet-exposed WS_FTP servers unpatched against a maximum severity vulnerability are now targeted in ransomware attacks.

1 week ago



OK GREAT.

HOW DO I PREVENT IT?

BEST PRACTICES

“No. Layers. Onions have layers. Ogres have layers. Onions have layers. You get it? We both have layers.”

- Shrek, 2001

BEST PRACTICES

1. PATCH MANAGEMENT

- Keep all systems and software up to date
- Malicious actors exploit outdated machines
- Critical security releases protect against attacks
- Signature-based security

2. BACKUP YOUR DATA

- 3-2-1 rule
- There should be 3 copies of your data.
- Your data should be in at least 2 locations.
- 1 of those locations should be offsite.
- Local device + secure cloud

BEST PRACTICES

MFA/2FA

- Multi-factor authentication or two-factor authentication
- Good double-check
- Extra step to verify it is you who has proper access

PASSWORD MANAGER

- Never forget a password again
- Eliminates repeat passwords
- If a hacker gets the one password you use for everything, they get the “keys to the kingdom”

EDUCATION

- Most attacks are due to human error
- Hackers’ method of choice is persuasive emails
- Phishing, spear phishing

MULTI-LAYERED SECURITY

FIREWALL

- First line of defense
- Your hardest working security device
- Zero-day threats

ENDPOINT SECURITY

- Antivirus
- Antimalware
- EDR
- Software Firewall
- Scans, Quarantine, and Flags

APPLICATION SECURITY

- Only use trusted applications on business network
- User Access & Permissions

NEXT-GENERATION ANTIVIRUS

Norton

McAfee

Traditional Antivirus

- Affordable
- Signature-based threat protection
- Lightweight
- Becoming easier to exploit

Microsoft Defender
for Endpoint

SOPHOS

Bitdefender

CROWDSTRIKE

HUNTRESS

SentinelOne

Endpoint Detection & Response (EDR)

- Built for ransomware protection
- AI-powered
- Detects threats based on activity, does not need to rely on signature records
- Future of cybersecurity

IT TEAM

INTERNAL

Helpdesk (Level I, II, III)

System Administrator

Network Engineer

CTO

EXTERNAL

MSP: Managed IT Services Provider

Consultant

CO-MANAGED

Combination of both

MANAGED IT SERVICES

IT is expensive in-house

- Avg. Helpdesk Support: $52,336/yr*
- Avg. Systems Administrator: $99,399/yr*
- Avg. Network/Cloud Engineer: $118,750/yr*

*Glassdoor reports 2022

No IT is not the answer either

- Your nephew can help you with your home Wi-Fi, but not your business' security
- Jim from accounting may be good with computers, but he is being paid to do accounting

Maintenance is CRUCIAL

- Someone needs to be maintaining all infrastructure, policy, and data
- If you are calling for help, it may be too late

No Surprises & Peace of Mind

- Let the experts handle IT so you can run your business
- Pay per user/month, flat fee

Q&A

McMANUS IT
SOLUTIONS

THANK YOU

KIERAN MCMANUS

+1 (315) 210-8798

Kieran@mcmanusit.com

WWW.MCMANUSIT.COM