“10 Ways for Any Firm to Stay Protected and Secured in Today’s Cyber Landscape”

Presented by:

Beits (Eitan) Livneh

GALLOP Technology Group

- Born and raised in Israel
- Served in the IDF/ Intelligence force
- Worked at a Microsoft Israel.
- Moved to AZ in 2000
- Married to Christina, and to his job
- Children: 4 (ages 16,18,18,18)
- Hobbies: Family trips, Coaching & playing Volleyball, Efficiency and automation

Microsoft

LEGAL TECHNOLOGY SOLUTIONS
Supporting Your Technology

📋 **Download the full checklist of top tools firms use:** GallopTechGroup.com/checklist

www.GallopTechGroup.com
480-614-4227

INTRODUCTION

Cybersecurity has become one of the most important risks facing law firms today—but it's often misunderstood. Most firms don't experience issues because they lack technology.
They experience issues because of small gaps—gaps in process, gaps in visibility, and most importantly, gaps in everyday behavior.

Law firms are uniquely exposed because of the type of data they handle—confidential client information, financial transactions, and time-sensitive legal work.

What we're going to focus on today is not technical complexity. It's clarity.

What actually creates risk, what actually reduces it, and what practical steps firms can take to stay protected and secure in today's cyber landscape.

THE HIDDEN RISK: EVERYDAY HABITS

- Clicking unknown links
- Reusing passwords
- Sharing access informally
- Skipping security steps "to save time"

"Most breaches don't start with hackers, they start with habits."

THE REALITY FOR LAW FIRMS

- Law firms are prime targets for cyberattacks
- Sensitive client data – high value
- Attacks are increasing in frequency and sophistication
- Even small firms are being targeted

WHERE MOST FIRMS GO WRONG

- Over-reliance on tools
- Inconsistent processes
- Lack of staff awareness
- No clear ownership of security

“Most breaches don’t happen because tools failed, they happen because processes or behaviors did.”

WHAT MOST FIRMS ASSUME VS. REALITY

Assumption	Reality
• We're too small to be targeted • We have IT, we're covered. • It won't happen to us	• Small firms are easier target • Tools don't prevent behavior • Most firms learn after an incident

CASE STUDY: SMALL LAW FIRM RANSOMWARE ATTACK

What Happened:

- A **small law firm (~20M revenue)** was targeted by ransomware
- An employee received an email that looked like a **trusted contact**
- The email was part of an **existing conversation thread**
- Employee opened the attachment → attack began

👉 The firm assumed the email was safe because it looked familiar

Source: https://www.cfc.com/en-gb/knowledge/resources/case-studies/uk-cyber-claims-case-studies/cyber-claims-case-study-law-firm-leakage/?utm_source=chatgpt.com

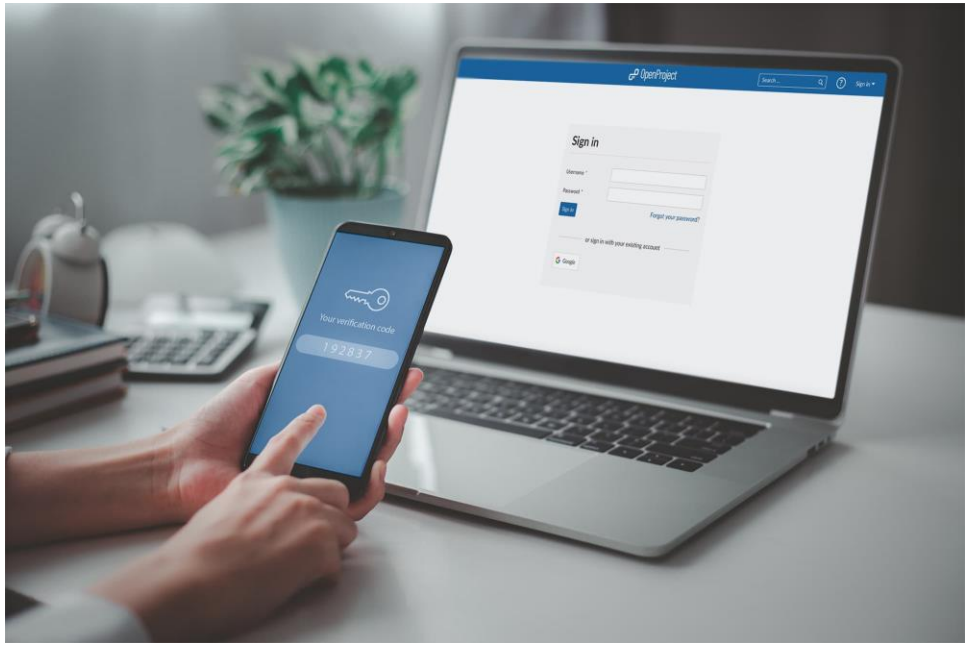
HOW ATTACKS ACTUALLY HAPPEN

- Email appears legitimate
- User clicks link or opens attachment
- Credentials are captured or malware is triggered
- Attacker gains access to email or system
- Attack spreads inside the firm

10 WAYS TO STAY PROTECTED AND SECURED

1. Multi-Factor Authentication (MFA)

- Protect accounts beyond passwords
- Required for email, cloud apps, remote access
- One of the most effective controls



2. Keep Systems Updated

- Enable automatic updates
- Patch operating systems and software
- Reduces known vulnerabilities

10 WAYS TO STAY PROTECTED AND SECURED

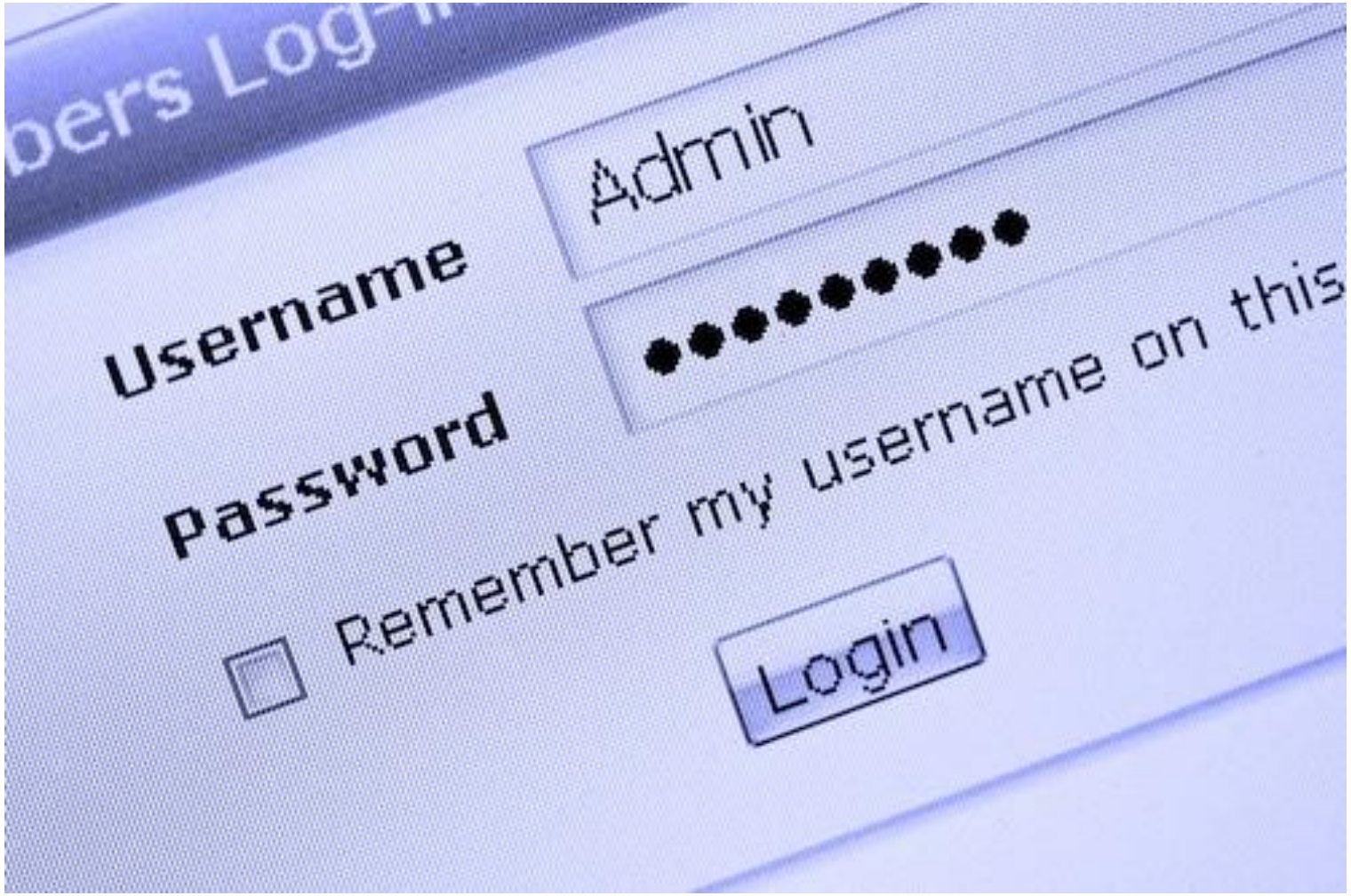
3. Staff Awareness & Phishing Training

- Most attacks start with email
- Train staff to spot suspicious messages
- Reinforce regularly

4. Secure Email Systems

- Prevent email spoofing
- Protect your domain reputation
- Reduce risk of impersonation attacks

Login Failed- please try again… and again… and again…



10 WAYS TO STAY PROTECTED AND SECURED

5. Access Control

- Limited access based on role
- Reduce exposure if accounts are compromised
- Review access regularly

6. Continuous Monitoring

- Detect threats early
- Respond quickly
- Visibility into activity across systems

10 WAYS TO STAY PROTECTED AND SECURED

7. Backup and Recovery

- Protect against ransomware
- Store backups securely
- Test recovery regularly

8. Secure Remote Work

-Protect remote access

-Secure devices used outside the office

-Enforce consistent policies

10 WAYS TO STAY PROTECTED AND SECURED

9. Clear Security Policies

- Define expectations
- Standardized processes
- Reduce human error

10. Align with Insurance & Compliance

- Meet cyber insurance requirements
- Strengthen overall security posture
- Improve incident readiness

CASE STUDY: Law Firm Ransomware Attack

Overview

A small U.S.-based law firm (under 50 attorneys) experienced a ransomware attack after an employee clicked a malicious email link.

What Happened

- An employee received a seemingly legitimate email
- The employee clicked a malicious link
- Ransomware spread across the firm's servers
- Critical systems and files became inaccessible

👉 *This happened during an active business week with deadlines and court-related work pending.*

Source: https://www.innovativecomp.com/wp-content/uploads/Case-Study-Law-Firm-Ransomware-Attack.pdf?utm_source=chatgpt.com

THE ROLE OF CYBER INSURANCE

- Insurance providers now require specific security controls (MFA, monitoring, training)
- Firms may be denied coverage or claims if requirements are not met.
- Security standards are increasingly driven by insurance expectations.
- Meeting this requirements strengthens overall protection, not just insurability.

“Insurance doesn’t replace security, it enforces it.”

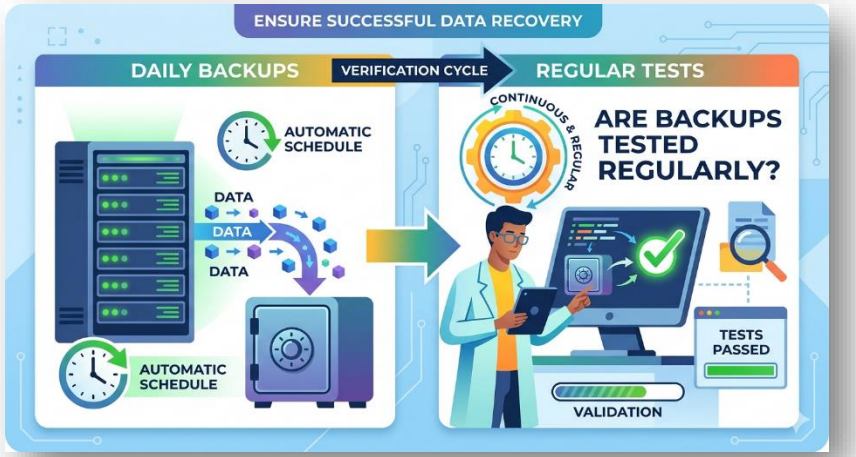
HOW CYBERSECURITY CONNECTS TO ETHICAL RESPONSIBILITIES

- Legal professionals have a duty to protect client confidentiality.
- Ethical obligations include maintaining reasonable safeguards for data.
- Cyber incidents can lead to ethical violations, not just operational issues.
- Responsibility extends beyond IT to firm leadership and daily practices.

"Cybersecurity is part of professional responsibility, not just technology."

QUICK SELF-ASSESSMENT

Do you use MFA everywhere?



Are backups tested regularly?

Do staff receive phishing training?

GALLOP Technology Group

Download the full checklist of top tools firms use: GallopTechGroup.com/checklist

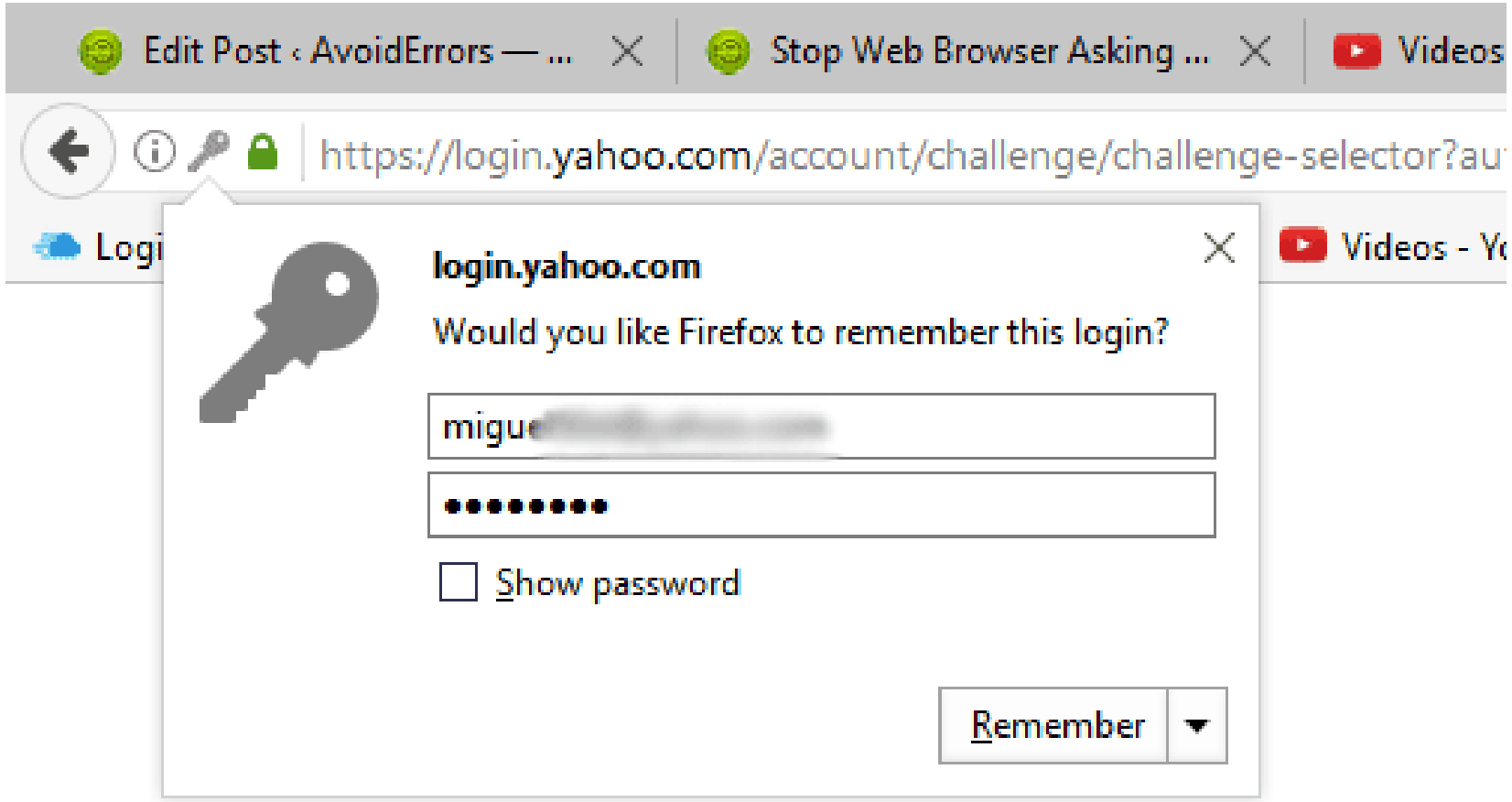
www.GallopTechGroup.com
480-614-4227

PRACTICAL TAKEAWAY

- Strong cybersecurity starts with the fundamentals, not complexity.
- The highest impact protections are often the simplest to implement.
- Most risk comes from inconsistent behavior, not lack of tools.
- Small gaps, repeated daily, create the biggest exposure over time.
- Progress comes from consistency, not one-time fixes.

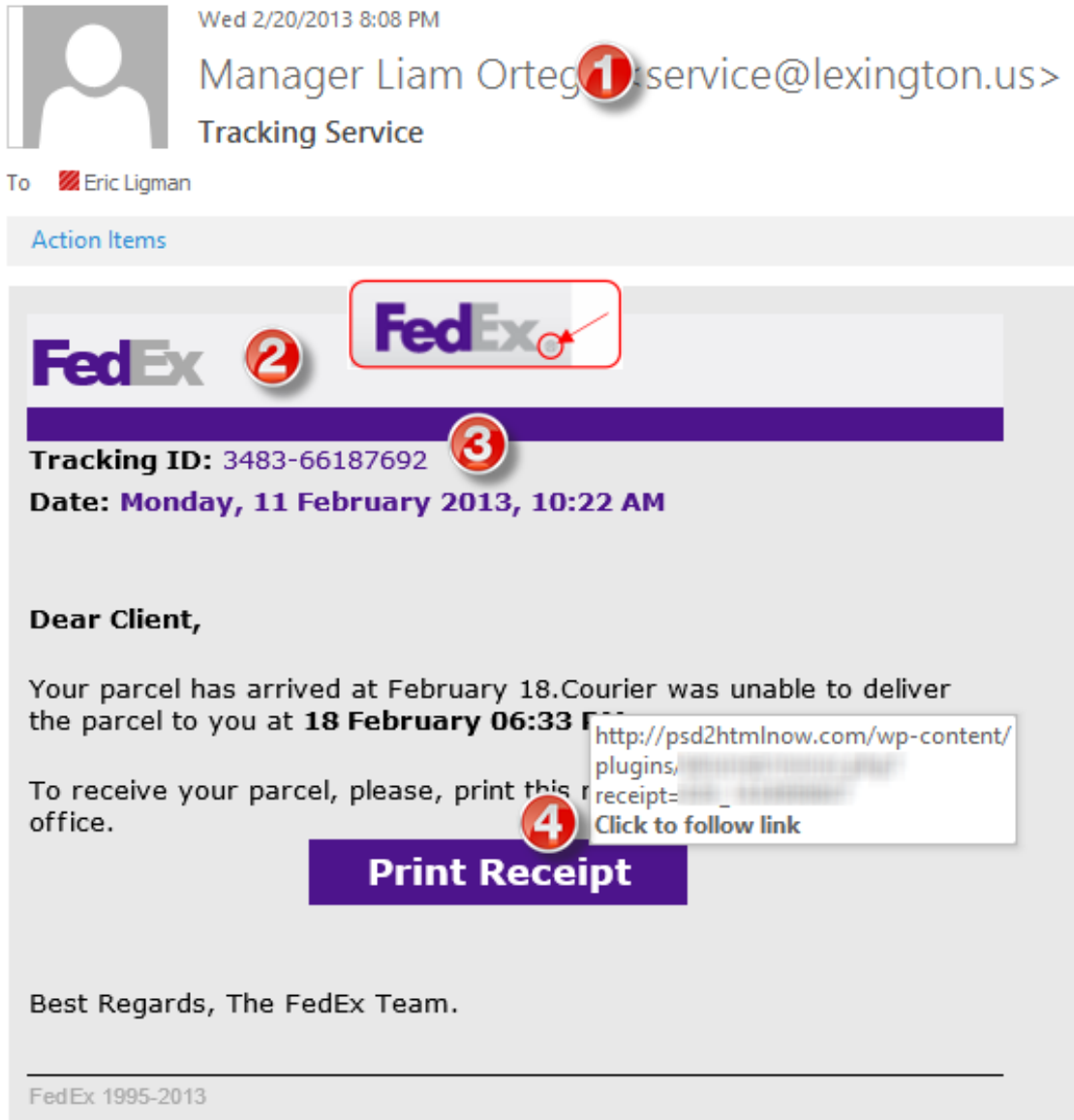
“Strong security is built through consistent actions, not advanced tools”

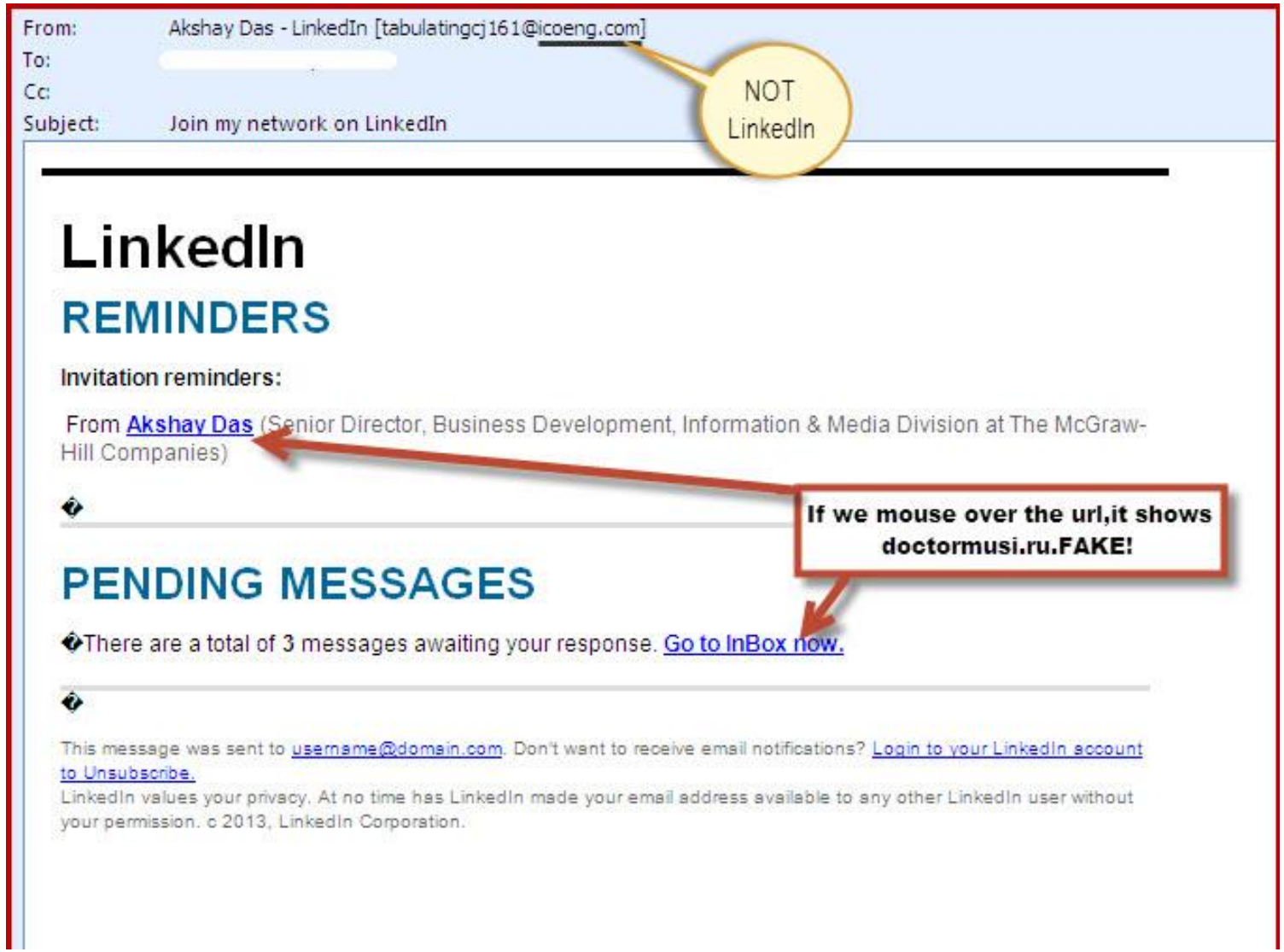
WHY NOT "remember password"? on Your Browser



Links: Tips

- Verify the sender
- Hover over links to see the URL (sometimes is appears at the bottom left of the screen)
- Do not click on links you cannot verify are 100% safe
- Type in the URL to the real website to login and verify the issue


Wed 2/20/2013 8:08 PM
Manager Liam Orteg service@lexington.us>
Tracking Service
To Eric Ligman
Action Items
FedEx
FedEx
Tracking ID: 3483-66187692
Date: Monday, 11 February 2013, 10:22 AM
Dear Client,
Your parcel has arrived at February 18.Courier was unable to deliver the parcel to you at 18 February 06:33
To receive your parcel, please, print this
office.
http://psd2htmlnow.com/wp-content/plugins/
receipt=
Click to follow link
Print Receipt
Best Regards, The FedEx Team.
FedEx 1995-2013


From: Akshay Das - LinkedIn [tabulatingcj161@icoeng.com]
To:
Cc:
Subject: Join my network on LinkedIn
NOT LinkedIn
LinkedIn
REMINDERS
Invitation reminders:
From Akshay Das (Senior Director, Business Development, Information & Media Division at The McGraw-Hill Companies)
If we mouse over the url,it shows doctormusi.ru.FAKE!
PENDING MESSAGES
There are a total of 3 messages awaiting your response. Go to InBox now.
This message was sent to username@domain.com. Don't want to receive email notifications? Login to your LinkedIn account to Unsubscribe.
LinkedIn values your privacy. At no time has LinkedIn made your email address available to any other LinkedIn user without your permission. c 2013, LinkedIn Corporation.

Attn: Your-150 Dollar Prime Credit Expires on 12/28. Shopper: [redacted] Spam x

Amazon Update <AmazonUpdate@efficaciouscrbays.xyz>
to me

Why is this message in Spam? It's similar to messages that were detected by our spam filters. Learn more

amazon.com Prime

The Amazon Marketplace

[redacted]

- - - - - -SHOPPER/MEMBER:4726
- - - - - -DATE-OF-NOTICE: 12/22/2015

Hello Shopper:[redacted]@gmail.com! To show you how much we truly value your years of business with us and to celebrate the continued success of our Prime membership program, we're rewarding you with-$100 in shopping points that can be used on any item on our online shopping site! (this includes any marketplace vendors)

In order to use this-$100 reward, simply go below to get your-coupon-card and then just use it during checkout on your next purchase. That's all there is to it!

Please visit-here now to get your reward

***DON'T WAIT! The Link Above Expires on 12/28!

Phishing Website

Phishing websites capture your login credentials to hack you

Some may download malware

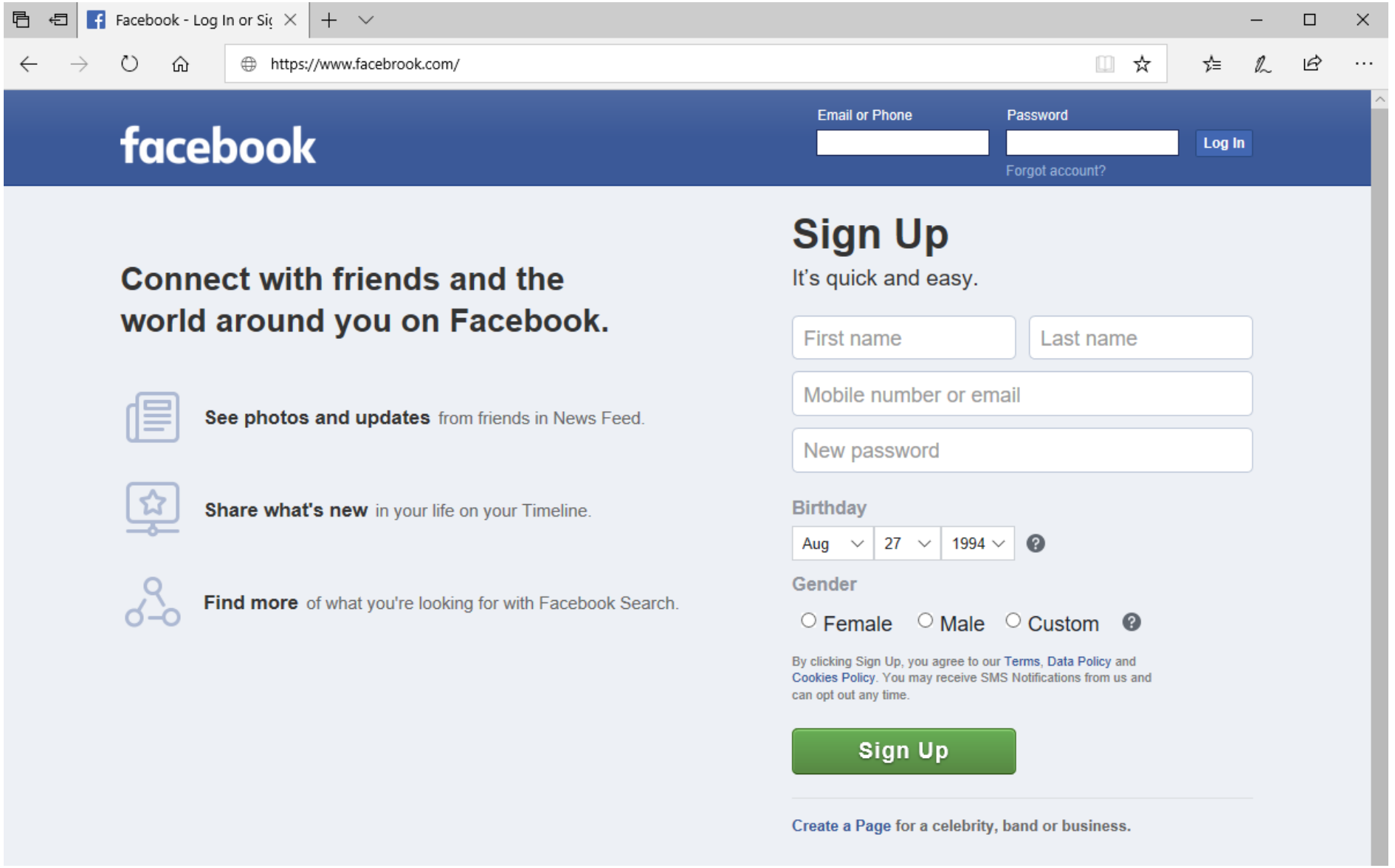
Some capture your IP address for an attack

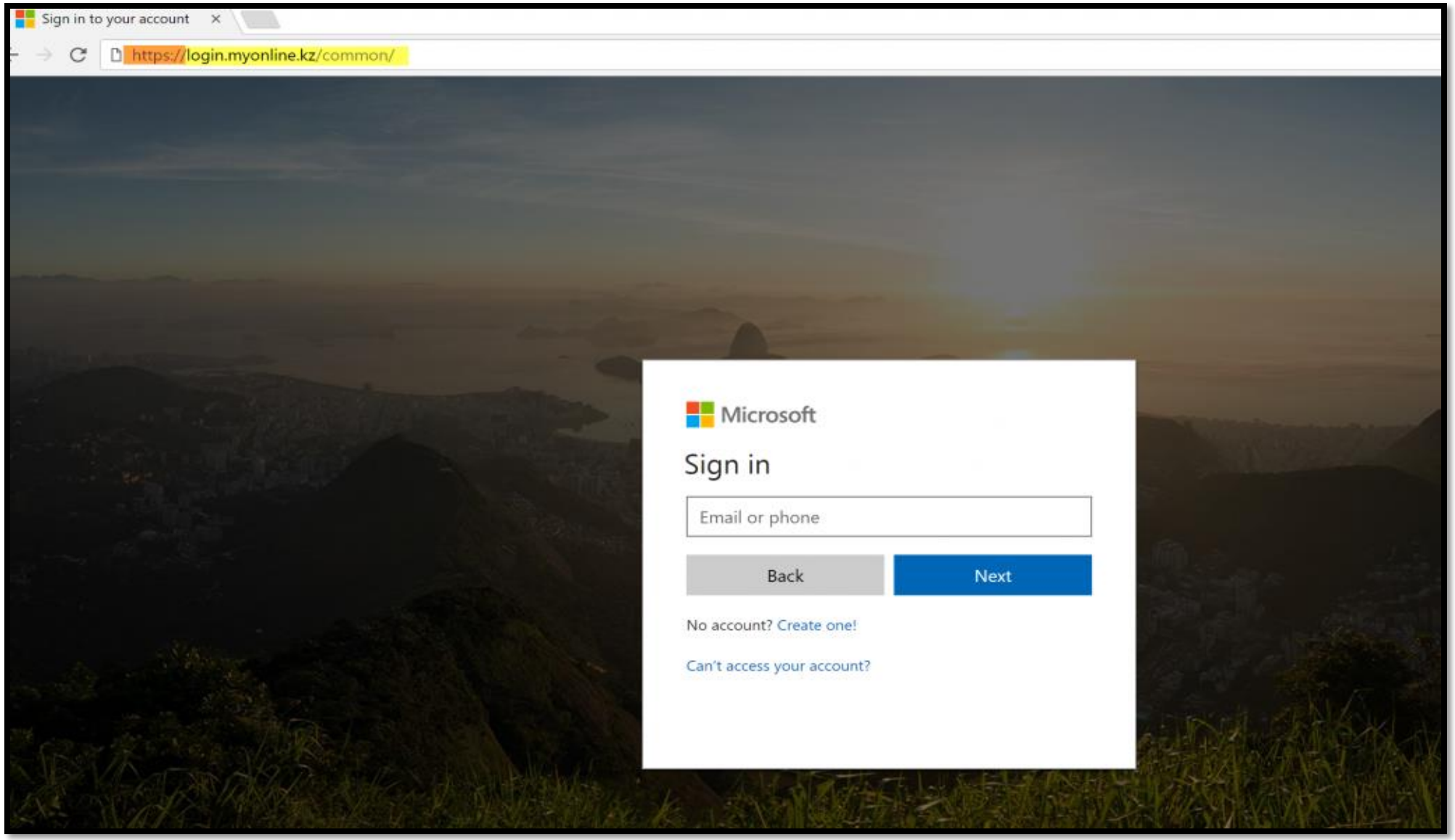
PHISHING WEBSITE

Phishing website: Detection

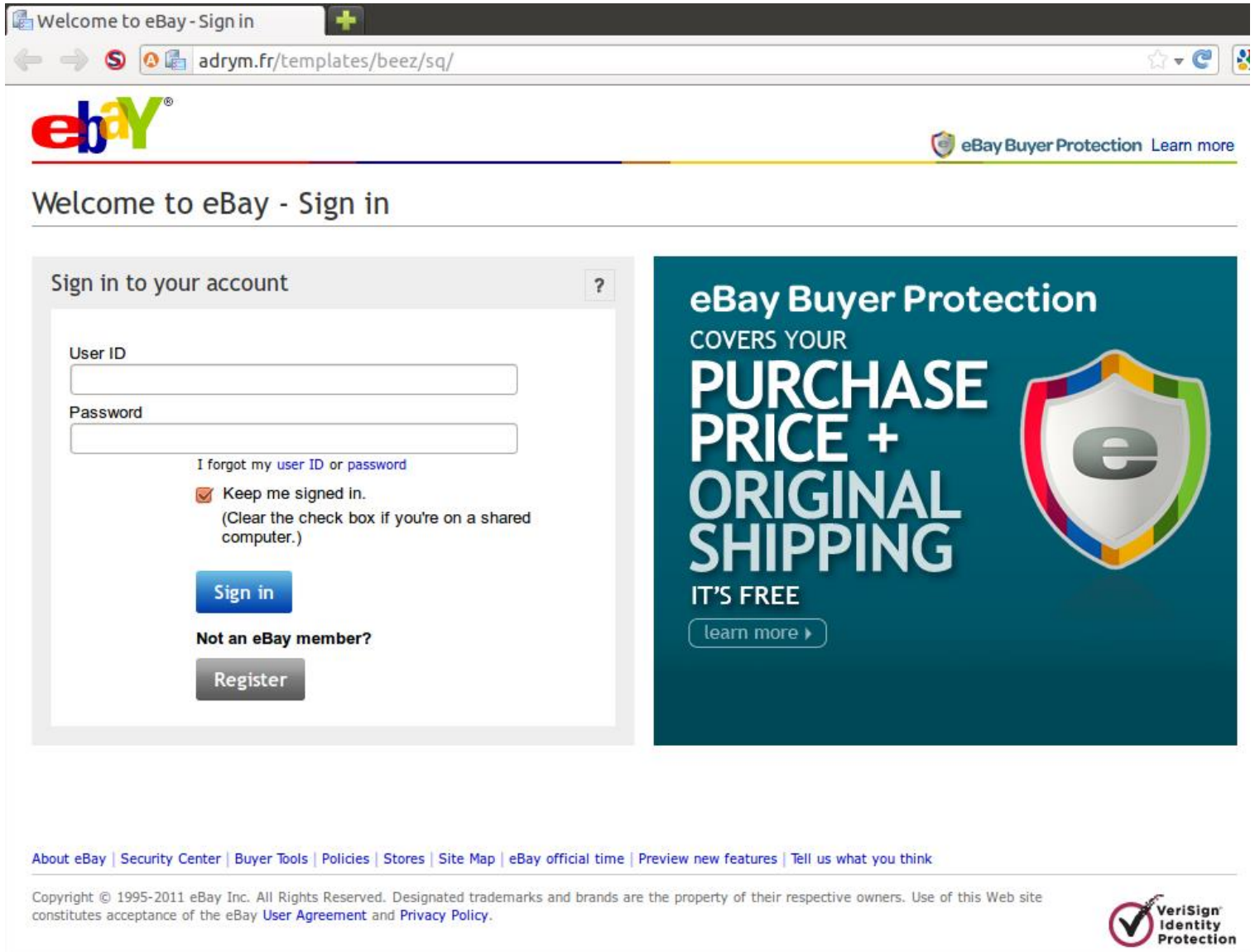
Fake websites are made quickly and have short lifespans, so look for:

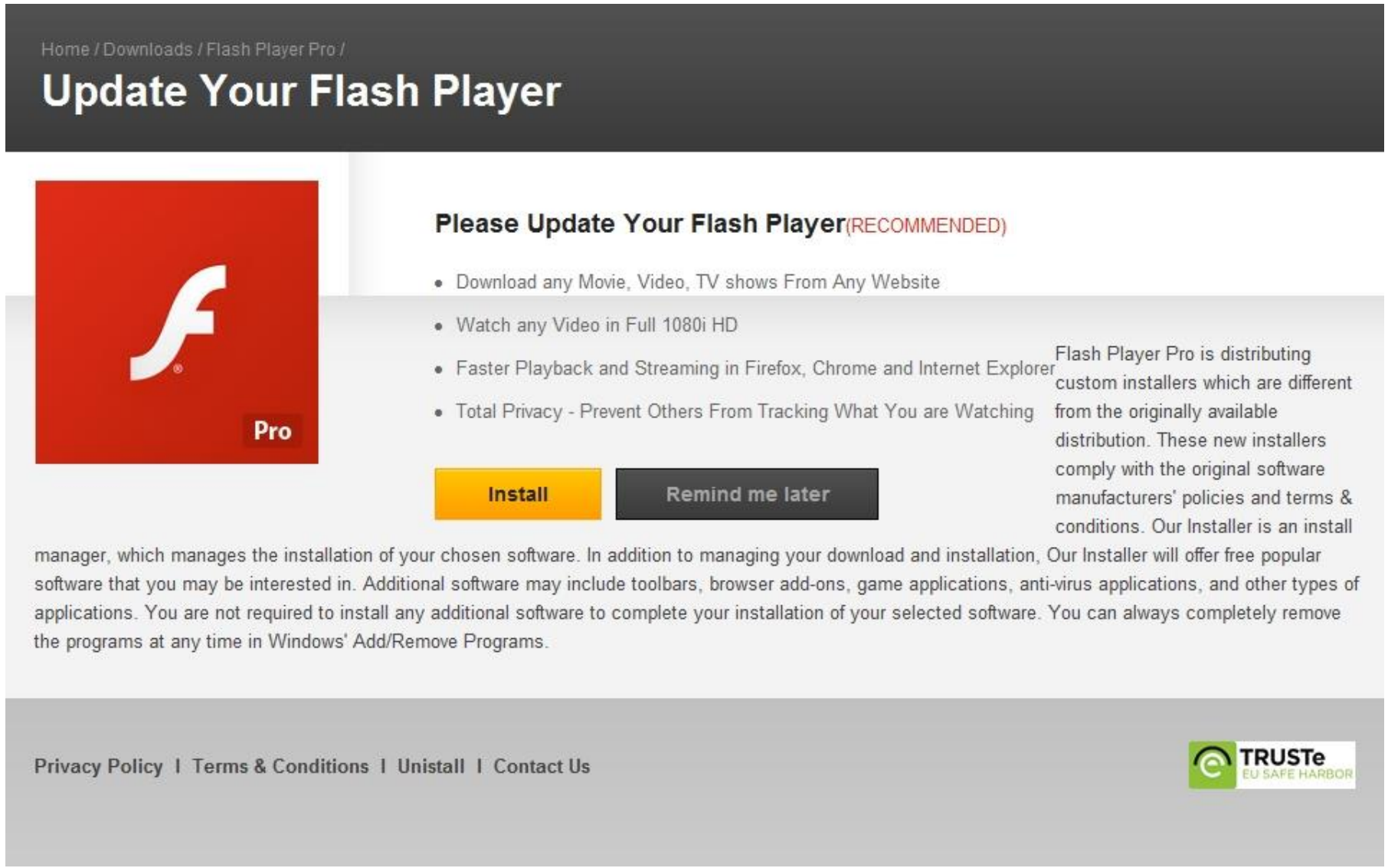
- Poor resolution in the logo, etc.
- Spelling errors
- Weird formatting
- SSL CERTIFICATE


Facebook - Log In or Sig
https://www.facebrook.com/
facebook
Email or Phone
Password
Log In
Forgot account?
Connect with friends and the world around you on Facebook.
See photos and updates from friends in News Feed.
Share what's new in your life on your Timeline.
Find more of what you're looking for with Facebook Search.
Sign Up
It's quick and easy.
First name
Last name
Mobile number or email
New password
Birthday
Aug
27
1994
Gender
Female
Male
Custom
By clicking Sign Up, you agree to our Terms, Data Policy and Cookies Policy. You may receive SMS Notifications from us and can opt out any time.
Sign Up
Create a Page for a celebrity, band or business.


Sign in to your account
https://login.myonline.kz/common/
Microsoft
Sign in
Email or phone
Back
Next
No account? Create one!
Can't access your account?

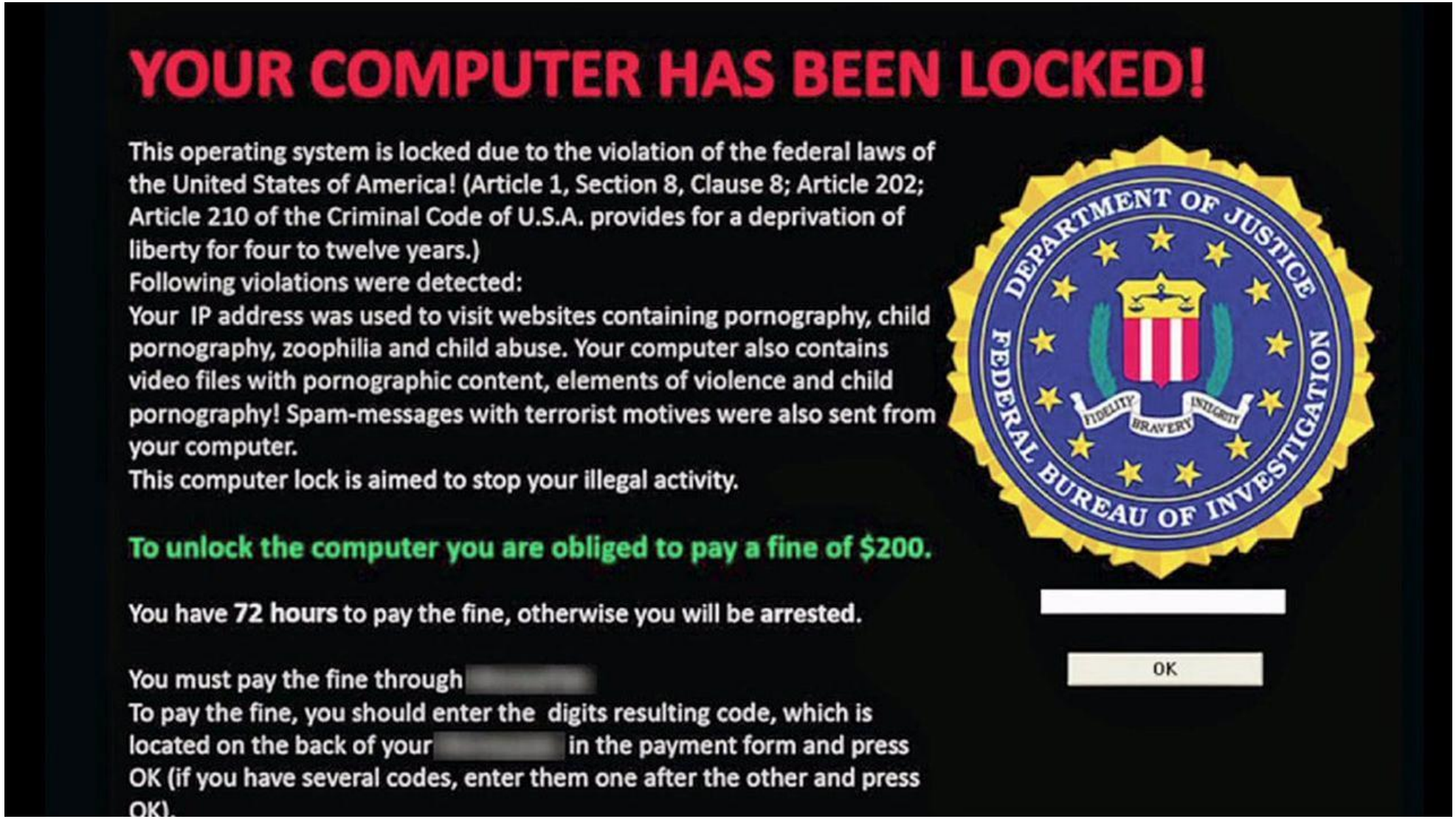

http://www.rfiimports.com/cpg146/albums/home/
Suspicious Website
Welcome - PayPal
PayPal
Welcome
Member Log-In
Email Address
Password
Suspicious website
This might be a phishing website.
Phishing websites impersonate trustworthy websites for the purpose of obtaining your personal or financial information.
Microsoft recommends that you do not give any of your information to such websites.
Report whether or not this is a phishing website.
What is Phishing Filter?
Shop Without Sharing
Your Financial Information
PayPal. Privacy is built in.
Learn more


Welcome to eBay - Sign in
adrym.fr/templates/beez/sq/
eBay Buyer Protection Learn more
Welcome to eBay - Sign in
Sign in to your account
User ID
Password
I forgot my user ID or password
Keep me signed in.
(Clear the check box if you're on a shared computer.)
Sign in
Not an eBay member?
Register
eBay Buyer Protection
COVERS YOUR
PURCHASE PRICE + ORIGINAL SHIPPING
IT'S FREE
learn more
About eBay | Security Center | Buyer Tools | Policies | Stores | Site Map | eBay official time | Preview new features | Tell us what you think
Copyright © 1995-2011 eBay Inc. All Rights Reserved. Designated trademarks and brands are the property of their respective owners. Use of this Web site constitutes acceptance of the eBay User Agreement and Privacy Policy.
VeriSign Identity Protection

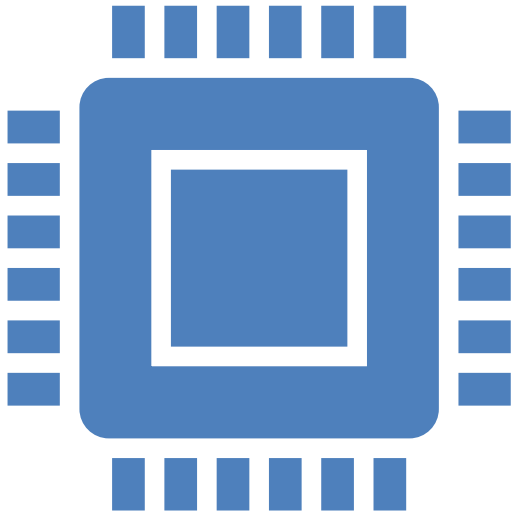

Home / Downloads / Flash Player Pro /
Update Your Flash Player
Pro
Please Update Your Flash Player(RECOMMENDED)
Download any Movie, Video, TV shows From Any Website
Watch any Video in Full 1080i HD
Faster Playback and Streaming in Firefox, Chrome and Internet Explorer
Total Privacy - Prevent Others From Tracking What You are Watching
Install
Remind me later
Flash Player Pro is distributing custom installers which are different from the originally available distribution. These new installers comply with the original software manufacturers' policies and terms & conditions. Our Installer is an install manager, which manages the installation of your chosen software. In addition to managing your download and installation, Our Installer will offer free popular software that you may be interested in. Additional software may include toolbars, browser add-ons, game applications, anti-virus applications, and other types of applications. You are not required to install any additional software to complete your installation of your selected software. You can always completely remove the programs at any time in Windows' Add/Remove Programs.
Privacy Policy I Terms & Conditions I Unistall I Contact Us
TRUSTe
EU SAFE HARBOR


CryptoLocker
Payment for private key
Choose a convenient payment method:
Bitcoin (most cheap option)
bitcoin
Bitcoin is a cryptocurrency where the creation and transfer of bitcoins is based on an open-source cryptographic protocol that is independent of any central authority. Bitcoins can be transferred through a computer or smartphone without an intermediate financial institution.
You have to send below specified amount to Bitcoin address 1KP72fBmh3XBRfuJDMn53APaqM6iMRspCh and specify the transaction ID, which will be verified and confirmed.
Home Page
Getting started with Bitcoin
Private key will be destroyed on
9/20/2013
6:48 PM
Time left
71 : 57 : 22
Enter the transaction ID and press «Pay»:
2 BTC
<< Back
PAY


Wana Decrypt0r 2.0
Ooops, your files have been encrypted!
English
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am
Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37
Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin ACCEPTED HERE
Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
Copy
Check Payment
Decrypt


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
To pay the fine, you should enter the digits resulting code, which is located on the back of your in the payment form and press OK (if you have several codes, enter them one after the other and press OK).
DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
FIDELITY
BRAVERY
INTEGRITY
OK

What To Do If You Have Ransomware?



- Disconnect:
  - If a computer or device is infected with ransomware, disconnect it from your network/files
  - Ensure your Backups are **not** currently running
  - Ensure Backups are disconnected from the network
- Report it:
  - Report the attack to your IT or CYBER SECURITY team

"REGULAR" ANTI VIRUS PROGRAM IS DEAD

- “Signature” files are not effective as they used to.
- AI is the new standard
- Backup files are easily wiped
- You’ll never spend as much as Amazon or Wells Fargo… Start small and make a huge difference

THREE COMMON TYPES OF ENCRYPTION

1. **Hard drive encryption**
    1. **Microsoft bitlocker or Apple FileVault**
    2. **Encrypts the entire hard drive, and unencrypts it when you log in**
    3. **This is not invasive BUT updates, hard restarts, power outages, and a bad hard drive can all cause your hard drive encryption to lock permanently. To mitigate damage, have a data restoration plan.**
2. **File encryption**
    1. **Axcrypt and Boxcryptor**
    2. **Encrypts specific folders or files**
    3. **Workflow will change when implementing one of these.**
3. **Email Encryption**
    1. **This encrypts individual emails**
    2. **The recipient must know the passcode to access the email**
    3. **The email only “lasts” for so long (ex: Deletes after a week)**

Cool Site

https://www.grc.com/haystack.htm

NEVER, EVER

Save your passwords on an excel spreadsheet or word document

Invest in a password manager software… WHY NOT?

REFERENCES & RESOURCES

- *Data Breach Investigations Report (DBIR)*
  https://www.verizon.com/business/resources/reports/dbir/
- *Formal Opinion 483 – Lawyers' Obligations After a Data Breach*
  https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/formal_opinion_483.pdf
- *NIST Cybersecurity Framework*
  https://www.nist.gov/cyberframework
- *CIS Critical Security Controls*
  https://www.cisecurity.org/controls
- *Formal Opinion 477R – Securing Communication of Protected Client Information*
  https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/aba-formal-opinion-477r.pdf
- *Phishing Guidance & Cybersecurity Best Practices*
  https://www.cisa.gov/phishing

We have created some great checklists for you… for free.

It will help you with:

- Streamline Compliance and Security
- Empowers Non-Technical Staff
- Save Time and Reduces Errors
- Support Business Continuity

To get your FREE checklists, visit:

https://GallopTechGroup.com/checklist (or scan the QR code)

GALLOP
Technology Group

www.GallopTechGroup.com
480-614-4227

Incident Response Plan Review (or our template…)

For leaders worried about what will happen on that bad day.

Why is it important?

- Identify Weaknesses
- Ensure Compliance
- Improve Response Time
- Enhance Team Preparedness
- Protect Your Reputation

To fill out the form for FREE IRP assessment:

https://www.galloptechgroup.com/incident-response-review/ (or scan the QR code)

GALLOP
Technology Group

www.GallopTechGroup.com
480-614-4227

Complementary Domain / Email security assessment
This protects your BRAND. Not just your SYSTEMS

Why is it important?

- Prevent Email Spoofing
- Protect Against Phishing Attacks
- Improve Email Deliverability
- Build Customer Trust
- Gain Insight into Email Activity
- Detect Leaked or Stolen Information

To request your FREE assessment, visit:

https://www.GallopTechGroup.com/free-domain-check (or scan the QR code)

GALLOP Technology Group

www.GallopTechGroup.com
480-614-4227

Hacking demo you should watch:

This is for teams who don't yet believe how simple attacks really are

Why?

- See how easy a hacker gains FULL access to a computer.
- See how simple social engineering can trick employees.
- See how fast your pictures or files can be stolen.
- See how simple hacker can capture your keystrokes.

To watch this video, visit:

https://GallopTechGroup.com/hacking-demo (or scan the QR code)

GALLOP Technology Group

www.GallopTechGroup.com
480-614-4227

Stay in touch

- Reach out to me directly with questions/ concerns
- Reach out to request a speaking engagement

My social links and contact information:
www.GallopTechGroup.com/Beits
Or scan the QR code

Download the full checklist of top tools firms use: GallopTechGroup.com/checklist