BVCC General Meeting

October* 14, 2024

"Protecting Yourself From Internet Cybercrime"

Joel Ewing

*** October is National Cybersecurity Month**

These slides will be published on the BVCC website
(Information ►Presentations)

Cybercrime Overview

- **How big is the Problem?**
- **How the bad guys attack**
- **What is their objective?**
- **How to defend yourself**
- **What if you become a victim?**

How Big Is The Problem

- **According to FBI, reported financial losses from cybercrime in 2023 was a new high of $12.5 billion**
  - **880,418 complaints received by FBI – much unreported**
  - **Investment fraud, corporate email compromise, ID theft, theft of online credentials, theft of sensitive information, ransomware/extortion, installation of malware to access sensitive information, or to use your computer to launch attacks on other computers and/or perform actions that are difficult to track back to perpetrator.**
  - **Internet crime is now big business, with some parties making a profit selling tools that less capable criminals use to commit the Internet attacks**
- **For a business, eliminating malware from a corporate network can cost many person-hours, and the effects of a successful attack on customer confidence can be irreparable.**
- **For a nation, vulnerable infrastructure is a national security risk**

How the Bad Guys Attack

- **Email spam –**
  - **Includes phishing (pretending to be from a person or company you trust). Forged From address, unknown senders – used to trick you into believing a dangerous email is safe.**
  - **May contain malware attachments, links to bad websites or bogus contact info. Uses social engineering designed to tempt you into taking action that puts you at risk.**
  - **HTML-format email can run scripts or download files that exploit security weaknesses even without user action. Email clients, like Thunderbird, by default can block HTML download of remote content.**
  - **"Innocent" emails can be the "hook" to begin follow-up contact for more complex scams.**

How the Bad Guys Attack

- **Rogue or compromised websites**
  - **"Drive-by downloads" – security bugs in your browser, installed browser extensions, or your Operating System may be exploited to download code to your machine without your consent.**
  - **Attractive links or downloads may download infected code (this is why you do research and only install applications from "trusted" websites).**
  - **Third-party adware is used by many websites (for revenue) and is an attractive target for attack. Some websites that I trust have at times had bogus "Your machine is infected" alerts that I suspect came from ad links on the website.**
  - **Bad guys use spam email to trick you into visiting bad websites, or set up enticing websites advertising cheap pirated goods or porn, because that tends to attract customers who are less cautious.**

How the Bad Guys Attack

- **Security bugs in Operating System services that are open to the network**
  - **A serious problem if you have a computer that is directly connected to the Internet with no router as a firewall – MS Windows has a long history of such exposures.**
  - **Even with a firewall, can be a problem. If one computer on your local network gets infected with malware, it can more-easily spread to other local computers as communication among local computers bypasses the router firewall.**
  - **Some routers even have security issues, making it possible to install malware on the router without any login. If the router code or its configuration is corrupted, that can then be used to attack computers on your home network. Never enable any router for "remote configuration" from the Internet, as that makes them more vulnerable to attack.**

How the Bad Guys Attack

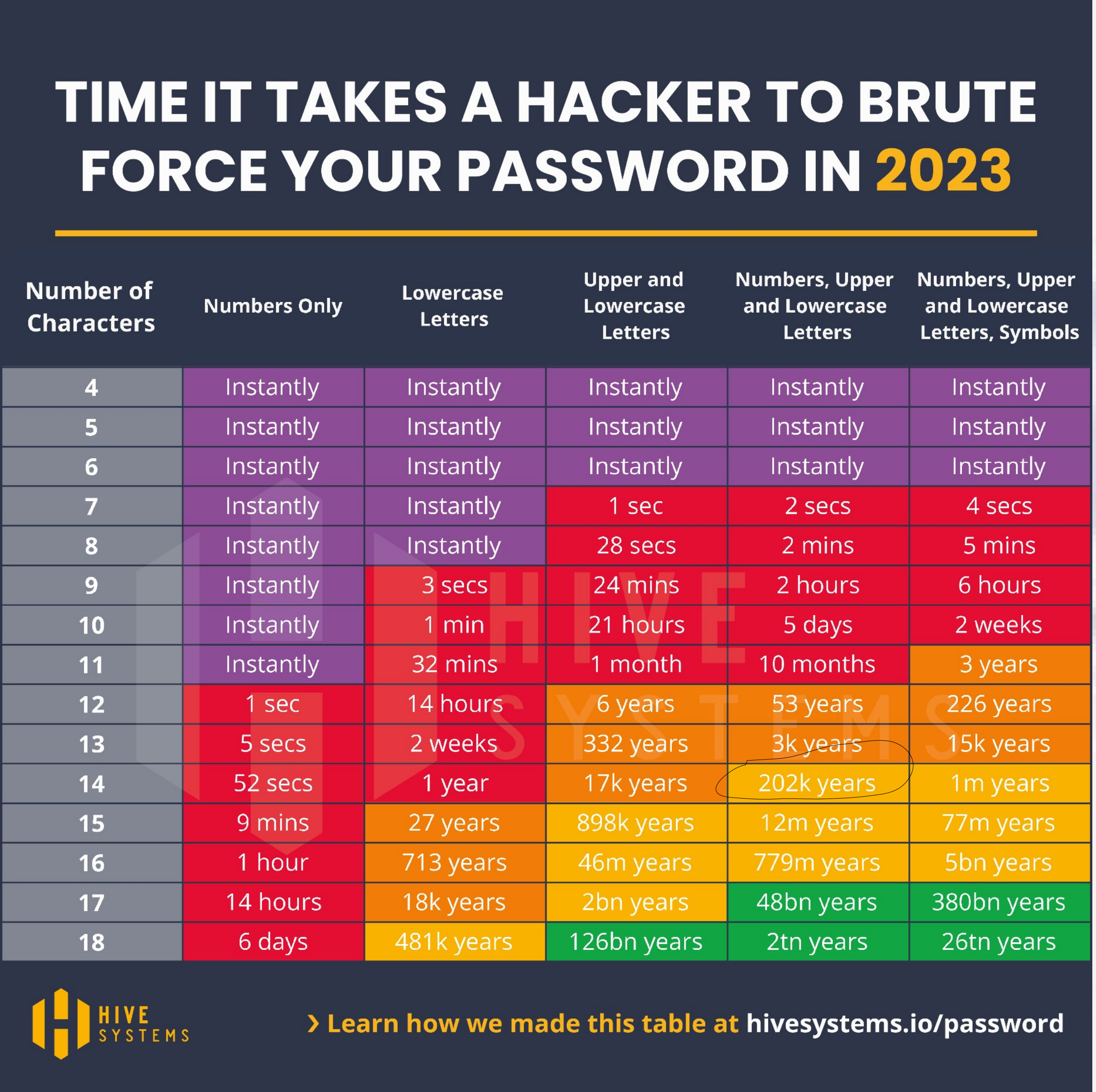
- **Telephone Initiated Attacks**
  - **I haven't seen one of these recently, but one of the simplest past social engineering attacks was a phone call claiming to be from some large company, such as from Microsoft Technical Support staff, claiming your computer is causing problems on the Internet and offering to fix it.**
    - **Typically they ask you to take actions on your computer that (if you are running Windows) will allow them to control your computer remotely. Once they have that, they can download and install malware on your computer that allows remote control of your computer to comprise your data from that point until all malware is removed.**

What Is The Objective?

- **To convince you to send them money by some method that is difficult to track or cancel**
- **To get partial control of your computer system**
  - **To steal your data to steal your identity and/or extort money**
  - **To use your system as a means to attack other systems on the Internet while hiding the real location of the attacker.**
- **It takes less work to claim to have compromised your system than to actually do it. Some claims are just bogus – an email or alert that provides contact info or links to resolve a problem may actually be an attempt to get you to act in a way that will install malware, or to get you to pay to resolve a problem that doesn't exist.**

How To Defend Yourself

- **Passwords for Online Accounts**
  - **Use different, strong passwords on all your online accounts, and use Multi Factor Authentication (MFA) when possible on sensitive accounts (financial accounts and email recovery accounts)**
    - **Random passwords best, but need a decent Password Manager**
    - **If MFA used, need multiple MFA methods (email accounts, mobile phones) to avoid single point of failure**
    - **Can use random combination of words – easier to type, but longer for same level of security (with 7771 words, 6-7 words roughly equiv to 14 random chars)**
    - **A suitably-strong password does not need to be changed after some fixed period – change only if there is a reason to suspect it might have been compromised.**



TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2023

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	1 sec	2 secs	4 secs
8	Instantly	Instantly	28 secs	2 mins	5 mins
9	Instantly	3 secs	24 mins	2 hours	6 hours
10	Instantly	1 min	21 hours	5 days	2 weeks
11	Instantly	32 mins	1 month	10 months	3 years
12	1 sec	14 hours	6 years	53 years	226 years
13	5 secs	2 weeks	332 years	3k years	15k years
14	52 secs	1 year	17k years	202k years	1m years
15	9 mins	27 years	898k years	12m years	77m years
16	1 hour	713 years	46m years	779m years	5bn years
17	14 hours	18k years	2bn years	48bn years	380bn years
18	6 days	481k years	126bn years	2tn years	26tn years

HIVE SYSTEMS

› Learn how we made this table at hivesystems.io/password

Keep in mind that around year 2000, many still found an 8 character password OK. Every year computation power available to hackers increases, gradually requiring longer passwords. For sensitive accounts today, I would suggest 14 chars.

Requiring numbers, upper and lower case letters is a reasonable password requirement. A few websites require special symbols. At best, this chart shows that only allows you to make the password one character shorter.

Time estimate is for random passwords. If pass phrase used, words must not be related and minimum of at least 20 chars.

How To Defend Yourself

- **Install Operating System and Application Updates When Available**
  - **Updates fix known Operating System security bugs and updates any built-in malware detection features (Windows Defender)**
  - **Current updates are more important in preventing malware than a slightly-better, third-party AntiVirus tool – most malware is designed to attack known software bugs in the hope of finding systems that haven't yet fixed the bug**

How To Defend Yourself – Email

- **The cheapest attack method, requiring low technical skills, is to reach your potential victims with spam emails.**
  - **There are tools and services for bulk emailing (legit and not), including lists of valid email accounts. Those that send fraud schemes are very difficult to stop – all it takes is a computer and an email sending service on the Internet that is not properly protected. The bad guys are constantly finding new ones.**
  - **The cost per email is so low that they only have to find a few victims every 100,000 emails for it to be profitable**
  - **I see 10 - 20 email fraud attempts per month per account on multiple email accounts that are "known" to spammers. Some of those emails are marked as SPAM, others not.**

How To Defend Yourself – Email

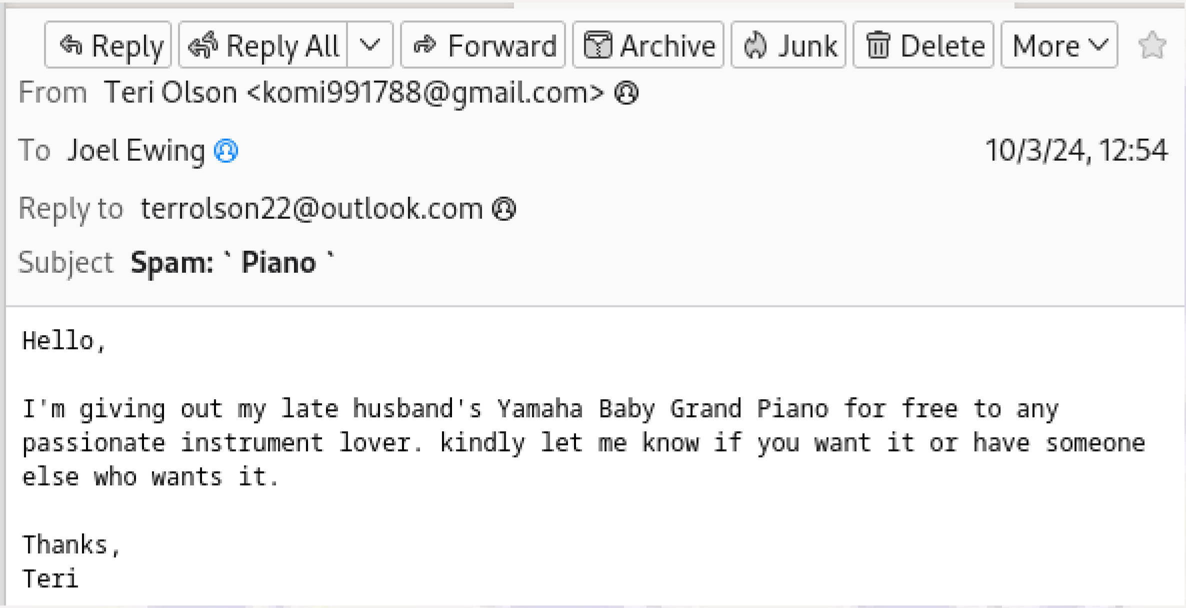
- **Regard all email with caution – don't trust links, contact phone numbers, email addresses, or attachments supplied in unexpected emails, even if they appear to be from known people.**
  - **Forged Email "From" names are trivial; forged From addresses also possible.**
  - **Offers of money, loans, jobs, etc. that "are too good to be true" are cons – attempts to steal ID info or get you to pay.**
  - **Invoices and claims that you owe money for items you haven't purchased, or to resolve a legal action against you are attempts to get info from you for ID theft or trick you into making unwarranted payments.**
  - **Attempts to extort money by claims they have embarrassing info on you – more likely a fraud, esp. if they omit any explicit proof they really have anything. It's much easier to send emails with that claim than to actually do what they claim.**

How To Defend Yourself – Email

- **Email "red flags"**
  - **The From address has the name of someone you know, but if you hover over the name, it is not from their usual email address**
  - **The email claims to be from a company, but the actual email address is clearly from a domain not associated with that company – companies don't use gmail or outlook email accounts.**
  - **There may be an overriding ReplyTo address that is questionable**
  - **Links in a email do not go to the company's domain name**
  - **The only way you are asked to respond is via telephone or by a link which goes to an unknown party.**
  - **Payment is requested in Bitcoin, by wire transfer, or by buying cash gift cards and supplying the numbers – these are means for rapid cash transfer that can be difficult to trace or reverse.**
  - **There is unusual urgency to act**
  - **The email is unsolicited "personal" communication from a major corporation or organization that doesn't communicate in that way – e.g., IRS only sends legal notices by US Mail, not by email or phone.**

Recognizing Different Types of Email Fraud

Offer of Free Expensive Item



From Teri Olson <komi991788@gmail.com>

To Joel Ewing 10/3/24, 12:54

Reply to terrolson22@outlook.com

Subject **Spam: ` Piano `**

Hello,

I'm giving out my late husband's Yamaha Baby Grand Piano for free to any passionate instrument lover. kindly let me know if you want it or have someone else who wants it.

Thanks,
Teri

If you play the piano and have always wanted, but could never afford, a baby grand, you know a good one may cost $25K, and might be tempted.

The odds are against someone unknown selecting you for this gift. Doing a Google search on Baby Grand fraud reveals this to be a con. You will find the piano is "in transit" with a moving company, so only a picture can be supplied; but for a significant fee ($1000) the moving company will go out of their way to deliver it to you.

After you pay the fee, there is no piano and contacts disappear.

Sextortion Email

From: Dane Potter <info@moneyforward.com>
To: editor@bvcomputerclub.org

Hello!
I am a hac ker who has access to your ope rating system.
I also have full access to your account.

I've been watching you for a few months now.
The fact is that you were infe cted with mal ware through an adu lt site that you visited.

If you are not familiar with this, I will explain.
Tr ojan Viru s gives me full access and control over a computer or other device.
This means that I can see everything on your screen, turn on the camera and microphone, but you do not know about it.

I also have access to all your contacts and all your correspondence.

Why your antiv irus did not detect mal ware?
Answer: My mal ware uses the driver, I update its signatures every 4 hours so that your anti virus is silent.

Email headers indicate the email was sent through "moneyforward.com", but from a London IP address that is not authorized to send email from that domain. The IP address may not be the originators IP, just a machine he controls.

AV software uses techniques more advanced than just virus signatures these days

I made a video showing how you sati sfy yourself in the left half of the screen, and in the right half you see the video that you watched.
With one click of the mouse, I can send this video to all your emails and contacts on social networks.
I can also post access to all your e-mail correspondence and messengers that you use.

If you want to prevent this,
transfer the amount of 1 300 USD (US dollars) to my bit coin address (if you do not know how to do this, write to Google: "Buy Bit coin").
My bit coin address (BTC Wall et) is:
bc1q85tjxpp3zzunvu4kkutzhpxv40ml53m4usff5n

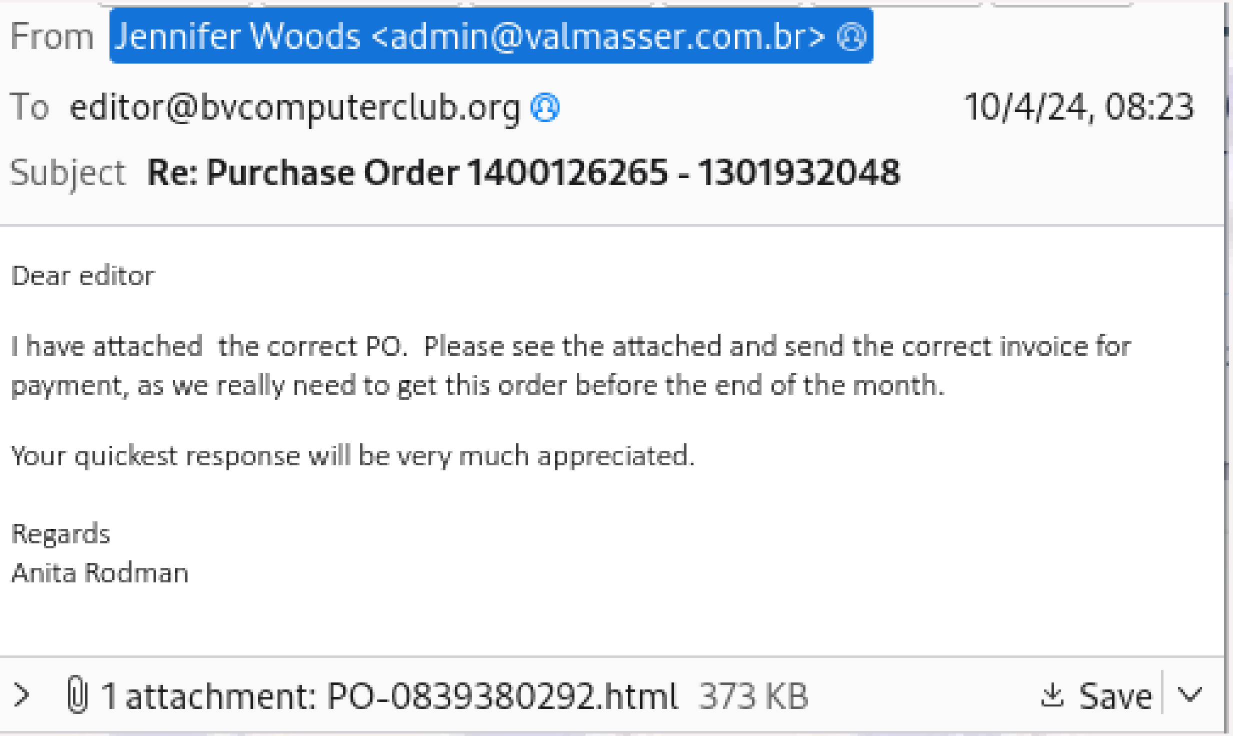
After receiving the pay ment, I will delete the video and you will never hear me again.
I give you 55 hours (more than 2 days) to pay .
I have a notice reading this letter, and the timer will work when you see this letter

Filing a complaint somewhere does not make sense because this email cannot be tracked like my bit coin address.
I do not make any mistakes.
If I find that you have shared this message with someone else, the video will be immedi ately distributed.

Best regards!

Note there is zero evidence given demonstrating he has obtained any actual data from your computer.
I know from the email accounts and computers involved, that no such info existed for him to steal.
The identical email was sent to multiple email accounts at BVCC. If you pay, there is nothing to correlate your payment with your email account, & no way to delete any associated video, which also implies there is no video.
Governments can track payments by seeing where the bitcoins go when transferred elsewhere – they eventually have buy some service associated with a name and address.

Fake Invoices



From Jennifer Woods <admin@valmasser.com.br>

To editor@bvcomputerclub.org 10/4/24, 08:23

Subject **Re: Purchase Order 1400126265 - 1301932048**

Dear editor

I have attached the correct PO. Please see the attached and send the correct invoice for payment, as we really need to get this order before the end of the month.

Your quickest response will be very much appreciated.

Regards
Anita Rodman

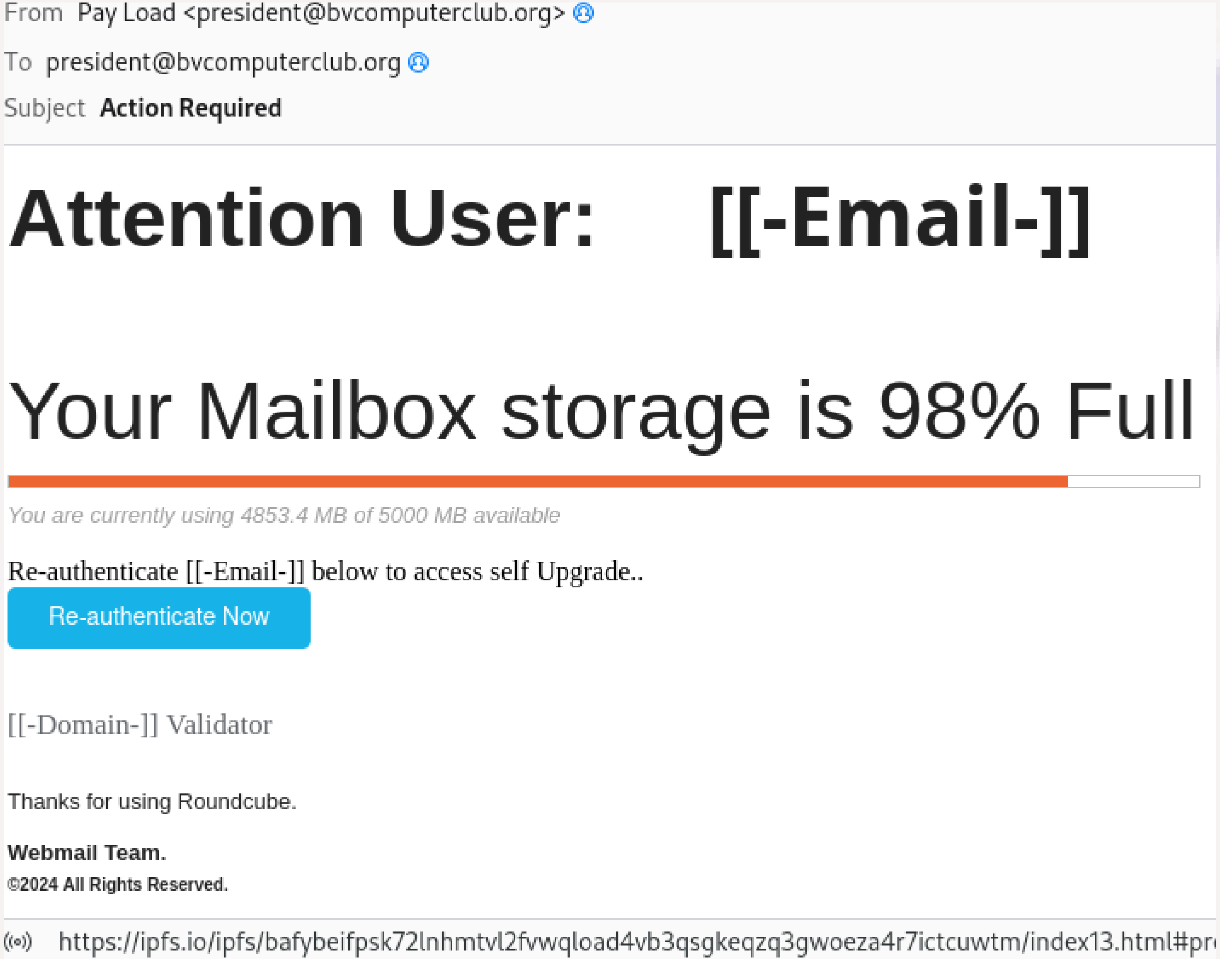
1 attachment: PO-0839380292.html 373 KB

The BVCC Editor has no budget, and wouldn't purchase items from Brazil (.br)

The sending account could be legit, but most likely is forged, because the headers show the sender's actual IP address to be located in Hungary.

Invoice might be in-line or as an attachment of some sort. Will probably suggest some form of contact and payment that is hard to track.
Domestic fake invoices frequently mimic invoices from well known American firms: McAfee, Amazon,...

Fake Problems With One Of Your Accounts



From Pay Load <president@bvcomputerclub.org>

To president@bvcomputerclub.org

Subject **Action Required**

Attention User: [[-Email-]]

Your Mailbox storage is 98% Full

You are currently using 4853.4 MB of 5000 MB available

Re-authenticate [[-Email-]] below to access self Upgrade..

[[-Domain-]] Validator

Thanks for using Roundcube.

Webmail Team.

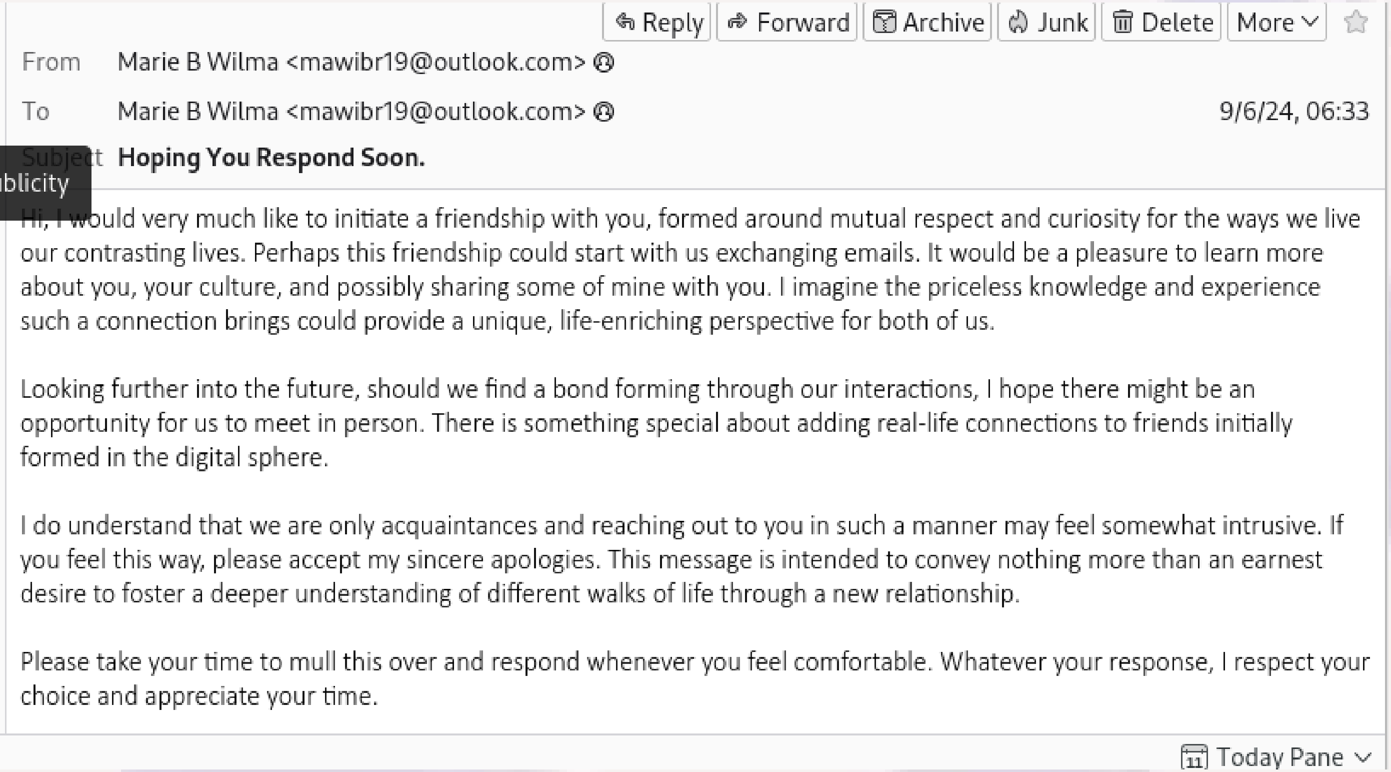
©2024 All Rights Reserved.

https://ipfs.io/ipfs/bafybeifpsk72lnhmtvl2fvwqload4vb3qsgkeqzq3gwoeza4r7ictcuwtm/index13.html#pr

In this case you need to know who is your email provider, as any warning on an email account should come from your email provider. For BVCC it is R4L.com – if legit, that should have been in the From address. There are several places where info seems to be missing. Hovering over the "re-authenticate" link shows it goes to ipfs.io, not to R4L.com. No doubt an attempt to steal email account credentials and/or get you to supply your CreditCard credentials.

And of course, going directly by trusted URL to you email provider allows you to verify there is no real problem.

Unsolicited "Friendships"



From Marie B Wilma <mawibr19@outlook.com>

To Marie B Wilma <mawibr19@outlook.com> 9/6/24, 06:33

Subject **Hoping You Respond Soon.**

Hi, I would very much like to initiate a friendship with you, formed around mutual respect and curiosity for the ways we live our contrasting lives. Perhaps this friendship could start with us exchanging emails. It would be a pleasure to learn more about you, your culture, and possibly sharing some of mine with you. I imagine the priceless knowledge and experience such a connection brings could provide a unique, life-enriching perspective for both of us.

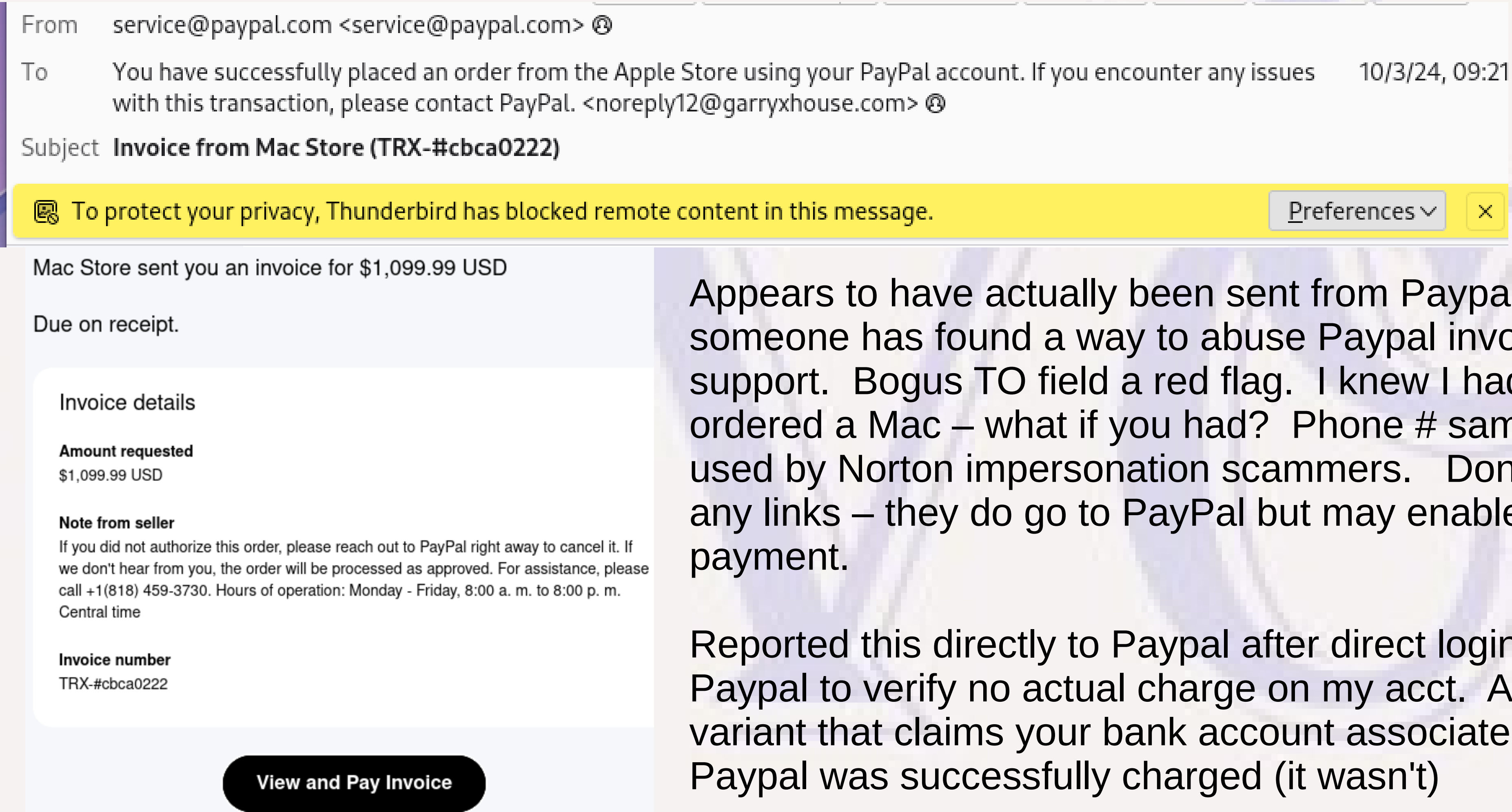
Looking further into the future, should we find a bond forming through our interactions, I hope there might be an opportunity for us to meet in person. There is something special about adding real-life connections to friends initially formed in the digital sphere.

I do understand that we are only acquaintances and reaching out to you in such a manner may feel somewhat intrusive. If you feel this way, please accept my sincere apologies. This message is intended to convey nothing more than an earnest desire to foster a deeper understanding of different walks of life through a new relationship.

Please take your time to mull this over and respond whenever you feel comfortable. Whatever your response, I respect your choice and appreciate your time.

Looks innocent enough, even warmly personal, until you notice you don't appear in the To address – meaning the same email was probably sent to 1000's of accounts, an action typical of a con artist.
Odds are high this is the beginning of a Romance Scam or Financial Investment Scam.
They are willing to spend months establishing a trusting relationship, then hit you for help in a fake financial crisis, or introduce you to a "lucrative" Investment Scam.

Bogus Paypal Invoice



From service@paypal.com <service@paypal.com>

To You have successfully placed an order from the Apple Store using your PayPal account. If you encounter any issues with this transaction, please contact PayPal. <noreply12@garryxhouse.com> 10/3/24, 09:21

Subject **Invoice from Mac Store (TRX-#cbca0222)**

To protect your privacy, Thunderbird has blocked remote content in this message.

Mac Store sent you an invoice for $1,099.99 USD

Due on receipt.

Invoice details

Amount requested
$1,099.99 USD

Note from seller
If you did not authorize this order, please reach out to PayPal right away to cancel it. If we don't hear from you, the order will be processed as approved. For assistance, please call +1(818) 459-3730. Hours of operation: Monday - Friday, 8:00 a. m. to 8:00 p. m. Central time

Invoice number
TRX-#cbca0222

Appears to have actually been sent from Paypal – someone has found a way to abuse Paypal invoice support. Bogus TO field a red flag. I knew I hadn't ordered a Mac – what if you had? Phone # same as used by Norton impersonation scammers. Don't trust any links – they do go to PayPal but may enable payment.

Reported this directly to Paypal after direct login to Paypal to verify no actual charge on my acct. Also saw a variant that claims your bank account associated with Paypal was successfully charged (it wasn't)

Large Unsecured Loan Offers

- **Various BVCC officers receive offers for pre-approved loans in the range $100K - $200K " based on the recent improvement in your Equifax business credit score, which has increased by <some number of points>"**
  - **Emails tend to show complete ignorance of to whom they are offering money, some indicate our business name as "Bits & Bytes", which is not a legal entity and has no assets that would warrant a credit score.**
  - **This is most likely a Personal Loan Scam – an excuse to probe for information that would be useful for ID theft, to gain access to your financial accounts, or to charge various fees for "processing" a nonexistent loan.**

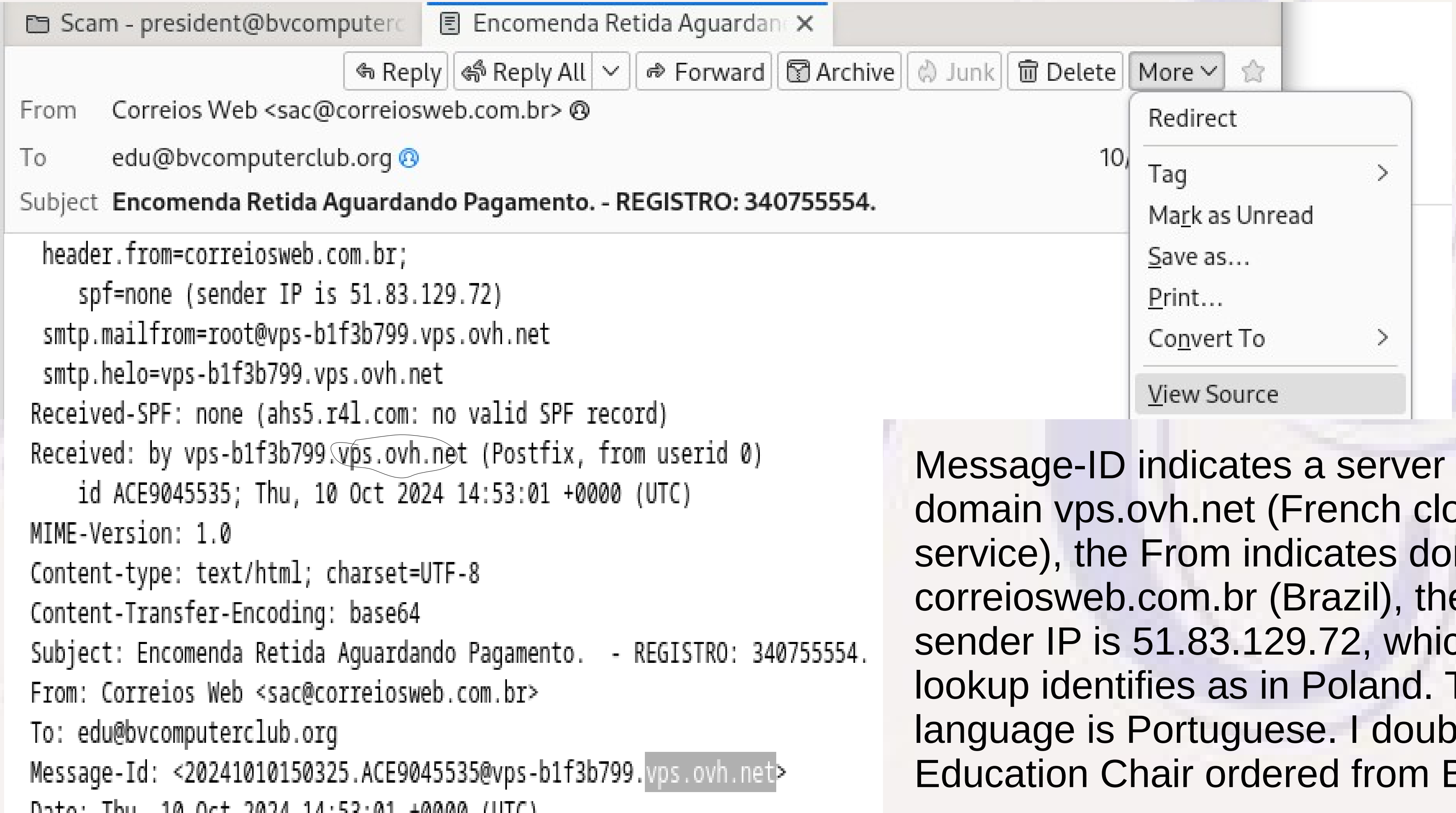
"Nigerian Prince" and Other Inheritance Scams

- **You have been selected to receive/transfer/invest a large sum of money**
  - **Because of death/persecution/imprisonment of person of wealth**
  - **Entrusting an unknown person (you), sight unseen, reputation unknown with his millions**
  - **They hope the prospect of receiving a large sum will result in the suspension of common sense – would you make such an offer if this were your money?**
- **Many variants – object is to get you to part with substantial transfer fees, legal fees, etc. to effect the imaginary transfer, or maybe to just get you to reveal personal info and financial info for ID and financial theft.**

Viewing Email Headers

- **As email is transported between servers, text lines called "Headers" are added to the top of the email to show how it is analyzed and routed**
  - **If you know what to look for, can provide clues on what server domain initiated the email into the Internet and the country origin of the computer that sent the email.**
  - **Only a few headers (From, Reply-to, To, Subject) are displayed by default, but email clients provide ways to view all headers**
    - **Thunderbird – while viewing mail, click "More" → "View Source"**
    - **Outlook – double click to view mail in separate window, then "Files" → "Properties"**
    - **Read headers from the bottom up (closest to Subject, From, To) for origin info**

Email Headers – Example (TB)



From Correios Web <sac@correiosweb.com.br>

To edu@bvcomputerclub.org

Subject **Encomenda Retida Aguardando Pagamento. - REGISTRO: 340755554.**

```
  header.from=correiosweb.com.br;
     spf=none (sender IP is 51.83.129.72)
  smtp.mailfrom=root@vps-b1f3b799.vps.ovh.net
  smtp.helo=vps-b1f3b799.vps.ovh.net
Received-SPF: none (ahs5.r4l.com: no valid SPF record)
Received: by vps-b1f3b799.vps.ovh.net (Postfix, from userid 0)
     id ACE9045535; Thu, 10 Oct 2024 14:53:01 +0000 (UTC)
MIME-Version: 1.0
Content-type: text/html; charset=UTF-8
Content-Transfer-Encoding: base64
Subject: Encomenda Retida Aguardando Pagamento.  - REGISTRO: 340755554.
From: Correios Web <sac@correiosweb.com.br>
To: edu@bvcomputerclub.org
Message-Id: <20241010150325.ACE9045535@vps-b1f3b799.vps.ovh.net>
Date: Thu, 10 Oct 2024 14:53:01 +0000 (UTC)
```

Message-ID indicates a server under domain vps.ovh.net (French cloud service), the From indicates domain correiosweb.com.br (Brazil), the actual sender IP is 51.83.129.72, which IP lookup identifies as in Poland. The language is Portuguese. I doubt our Education Chair ordered from Brazil.

How To Defend Yourself – Web Browsers

- **Edge by default interfaces with MS Windows Defender to block access to known bad websites and protect against some malware**
- **On Chrome browser, go to Extensions→ Visit Chrome Web Store, and install "Microsoft Defender Browser Protection" for extra protections**
- **For Firefox browser, There are some built-in protections, but no special extension for MS Defender.**
- **Don't install/enable browser extensions you don't use and occasionally check for extensions you didn't intend to install.**
  - **Rogue extensions are one avenue for browser malware attacks**
  - **Extensions from 3rd-party sources may not be as carefully tested**

How To Defend Yourself – Web Browsers

- **Do you need Alternative Third-party malware defenses such as Malwarebytes Premium (one of the better non-free tools)?**
  - **Advertising suggests it may be better in some areas than Windows default protections.   Reviews seem to be inconclusive.**
- **Keep in mind that no protection is 100% effective.**
- **Best protection is to deal with sites you know correspond to your financial institutions, utilities, retail stores, and be cautious with any new websites.**
- **Don't allow websites to install anything unexpected**

How To Defend Yourself – Web Browsers

- **Avoid using links in unsolicited emails**
- **Avoid websites with questionable content**
- **Avoid debit cards for online payment – direct payments can be disputed, but you are without the money unless and until the charge is resolved**
- **Services like PayPal can be used to minimize the number of online retail sites that have direct access to your credit card information**

How To Defend Yourself – Web Browsers

- **Adware content on websites can be a target for attack (successful attack on an ad source can affect multiple websites)**
  - **Pop Up windows that claim you have a problem may be bogus**
  - **If browser is locked up with a "serious" alert, take a picture of the alert and see if you can terminate the browser with ALT+F4**
  - **While it is possible to exploit security bugs from a browser, it is easier and more common to claim damage has been done than to actually do the damage claimed.**

What If You Become a Victim?

- **If you have fallen victim, report actual losses to FBI and local law enforcement. You may not be able to get your money back, but you may provide info that will help protect others and eventually enable catching the perpetrator.**
- **Law enforcement is not generally interested in email fraud attempts that were unsuccessful (there are just too many of them to pursue, even though technically each instance is still "wire fraud"). The Federal Trade Commission may be interested in tracking attempts, although as a matter of practicality I probably would only spend my time for ones that are repeated.**

Reporting Internet-Based Fraud Loss to FBI

- **If you are reporting Internet-based fraud, please submit a tip to IC3.gov (the FBI Internet Crime Complaint Center), which forwards complaints to relevant enforcement agencies..**
- **Be specific when providing information. Example: If reporting online criminal activity, please provide details such as website's URL or Internet address, the application name the communicated the fraud, date/time of the post, etc.**
- **Submit your information only once – don't expect any followup communication. Cases frequently aggregated together, not handled individually.**

Reporting Internet-Based Fraud Loss to FBI

- **Because of payment methods, the odds are not good you will get your money back, but there have been notable exceptions.**
  - **If you report losses promptly with enough detail, there have even been cases where cybercurrency payments were partially recovered. (exchanges vs personal wallet)**
  - **Even if you fail to recover your loss, you may save someone else from becoming a victim.**

Reporting Fraud to the FTC

- **ReportFraud.ftc.gov**
  - **Don't have to be a victim to report**
  - **Collects statistics on types of fraud to establish trends**
  - **Objective is to provide a record and examples of types of fraud so others can recognize them or search to confirm an overture is a fraud and not become a victim.**

Questions