The Daily Scam Newsletter - October 16, 2019

The Week in Review

In the last week we heard from two people who asked us about an extortion threat they had received via email. We assured them that the email was sent blindly to tens of thousands of people. But how is it, they asked us, that they know an old password I used to use? Criminals are crawling stolen password databases on the dark web and including that stolen information in the emails they send to people. It makes the threat appear so much more authentic and possible! But the email is completely fake. The sender hasn't installed malware on your computer and isn't monitoring you. He is simply using stolen information found on the dark web and has created a clever ruse.

By the way, If you want to know if YOUR EMAIL ADDRESS and PASSWORDS have been stolen from services on the Internet, visit "Have I been pawned?" Once there, enter your email address into the search field and read the results carefully. If you discover that your passwords have been stolen, it's time to change them everywhere they are used, not just the hacked site/service from which they were stolen. For tips to create a strong set of passwords that are easy to remember, visit our article on the topic!

From: <friedrich@bernaunet.de>
Date: Thu, Sep 12, 2019 at 2:14 PM
Subject: Security Notice. Someone have access to your system.
To: [redacted]

Hi!

I am a hacker who has access to your operating system.
This means that I have full access to your account: At the time of hacking your account([redacted]) had this password: beef89

You can say: this is my, but old password!
Or: I can change my password at any time!

Of course! You will be right,
but the fact is that when you change the password, my malicious code every time saved a new one!

I've been watching you for a few months now.
But the fact is that you were infected with malware through an adult site that you visited.

If you are not familiar with this, I will explain.
Trojan Virus 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 from e-mail and messangers.

Why your antivirus did not detect my malware?
Answer: My malware uses the driver, I update its signatures every 5 hours so that your antivirus is silent.

I made a video showing how you satisfy 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 $730 to my bitcoin address (if you do not know how to do this, write to Google: "Buy Bitcoin").

My bitcoin address (BTC Wallet) is: 1J1cFns1zZo5YZbMjVt93vVzzp7QeSJMNf

After receiving the payment, I will delete the video and you will never hear me again.
I give you 48 hours to pay.
I have a notice reading this letter, and the timer will work when you see this letter.

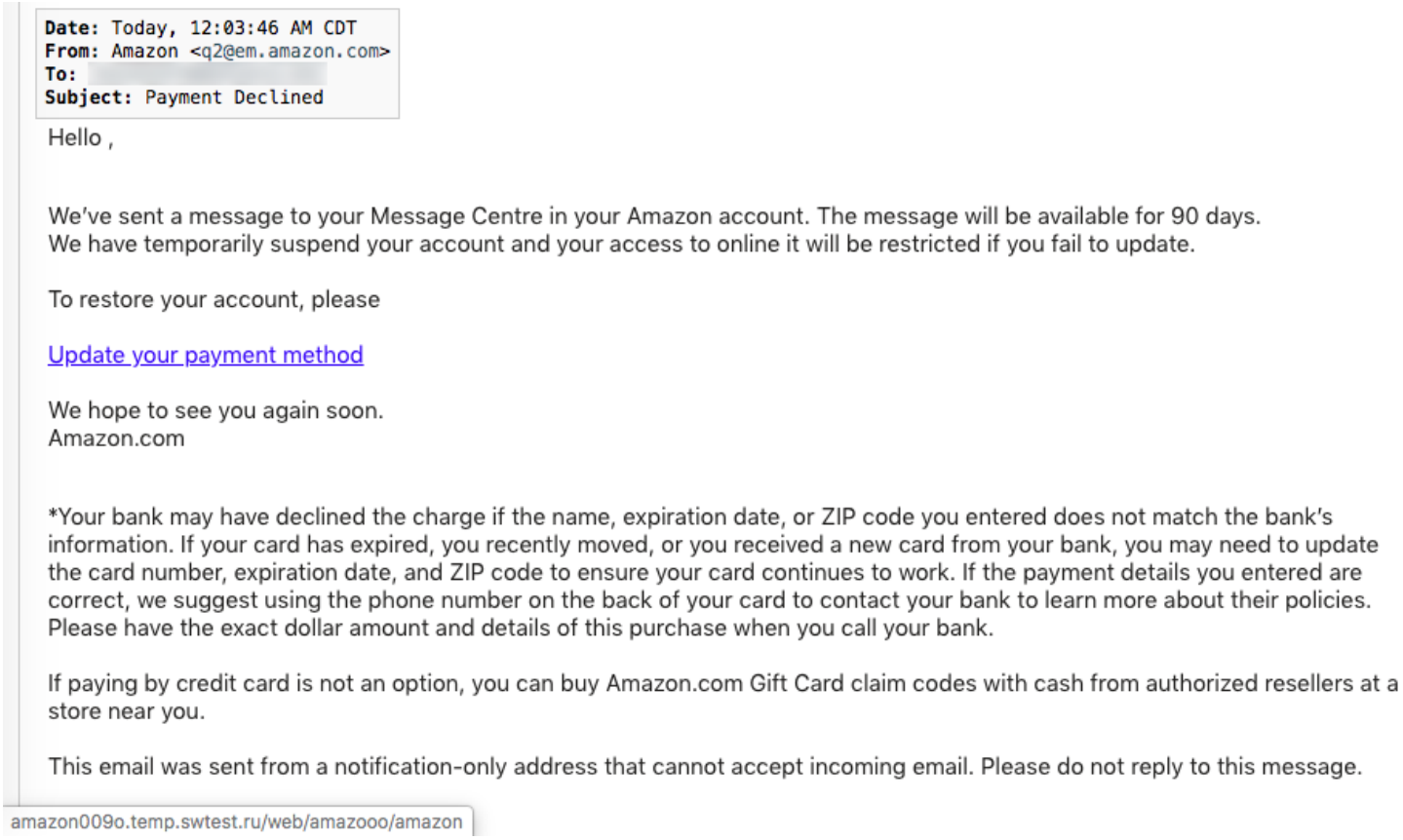
Filing a complaint somewhere does not make sense because this email cannot be tracked like my bitcoin address.
I do not make any mistakes.

If I find that you have shared this message with someone else, the video will be immediately distributed.
Bye!

Phish Nets: Amazon and Apple Accounts

This came from one of our readers. “We have temporarily suspend your account…” Notice the grammar error? This email contains several errors and they are the most important first tip that this isn’t legitimate. The criminals who created it correctly spoofed the FROM email address as **amazon.com**.

The real proof of this fraud comes from mousing over the link to “update your payment method” (without clicking!) to reveal where it points. Though you may see the name “amazon” twice in that link, along with another “amazooo,” this link actually points to a website in Russia. Notice the 2-letter country code “.ru” in the link!



Date: Today, 12:03:46 AM CDT
From: Amazon <q2@em.amazon.com>
To:
Subject: Payment Declined

Hello ,

We've sent a message to your Message Centre in your Amazon account. The message will be available for 90 days.
We have temporarily suspend your account and your access to online it will be restricted if you fail to update.

To restore your account, please

Update your payment method

We hope to see you again soon.
Amazon.com

*Your bank may have declined the charge if the name, expiration date, or ZIP code you entered does not match the bank's information. If your card has expired, you recently moved, or you received a new card from your bank, you may need to update the card number, expiration date, and ZIP code to ensure your card continues to work. If the payment details you entered are correct, we suggest using the phone number on the back of your card to contact your bank to learn more about their policies. Please have the exact dollar amount and details of this purchase when you call your bank.

If paying by credit card is not an option, you can buy Amazon.com Gift Card claim codes with cash from authorized resellers at a store near you.

This email was sent from a notification-only address that cannot accept incoming email. Please do not reply to this message.

amazon009o.temp.swtest.ru/web/amazooo/amazon

The next email was also spoofed to appear as though it came from apple.com. Subject line is “Important information regarding your Apple account.” Mousing over “UPDATE HERE” clearly shows that the link points to another link shortening service called Brevis. The link does not point to Apple.com! DEEEEELEEEETE!

From: Apple <n0reply.0yqvxr@qanz2kbom9.apple.com>
Date: October 9, 2019 at 10:45:02 AM EDT
To: [redacted]
Subject: Important information regarding your Apple account

Hello,
We're having some trouble with your current billing information.
Unfortunately, we could not charge you for your account.

Please verify your account information now, or your account will be locked permanent soon.

UPDATE HERE

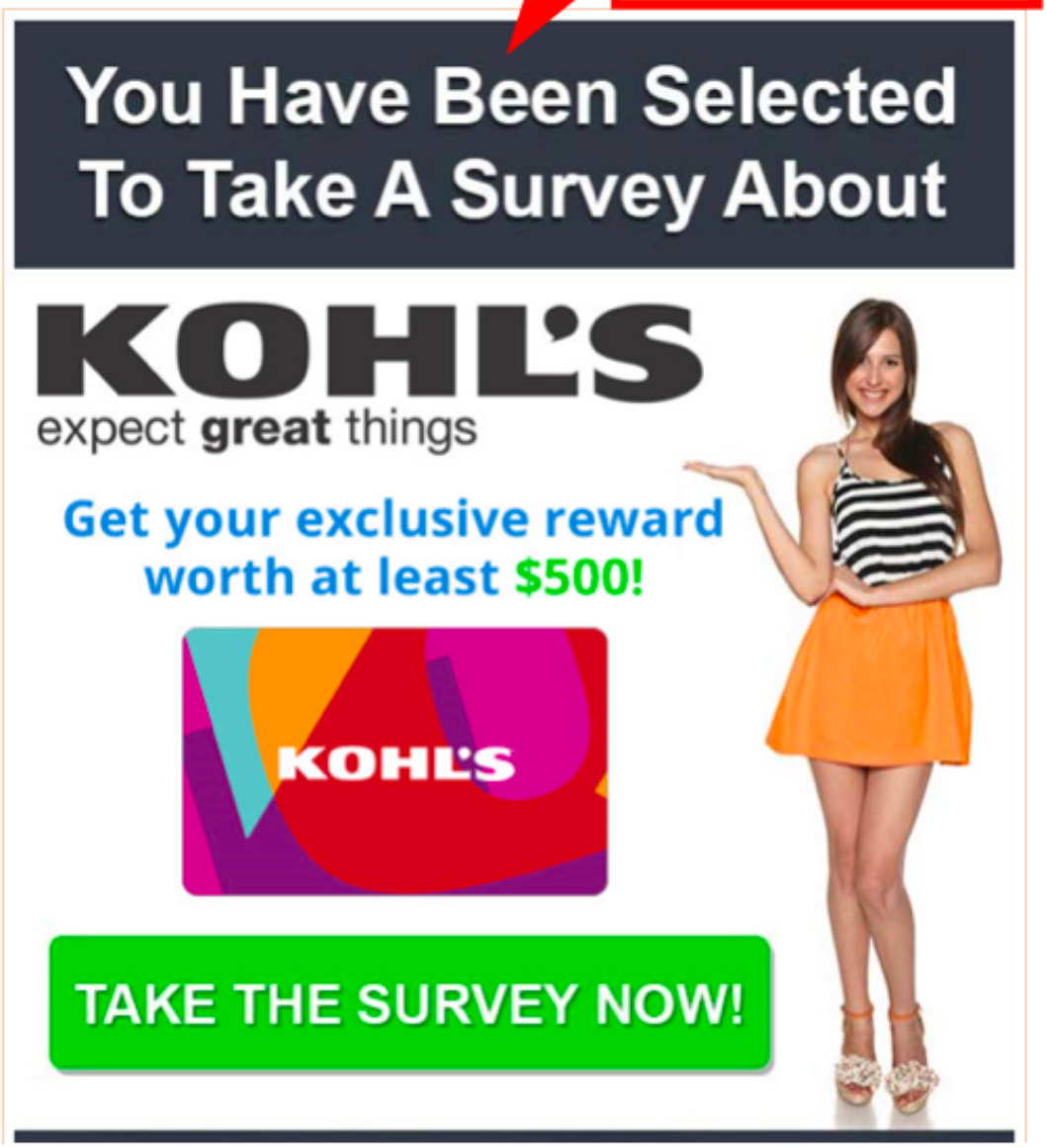
This email was sent from a notification-only address that cannot accept incoming email. Please do not reply to this message.

https://bre.is/AHdWywhu

Your Money: Kohls Survey again and Text About Shark Tank
This email came to one of our readers from a website in Australia and contains links that point back to another website registered in Australia. Notice in the FROM address and link the 2-letter country code ".au" = Australia. The domain that sent the email is called **"damage noise exposure" .com.au** while the links point to **"tumultuous trade tensions" .com.au**. After being hit with malware, this tumultuous website sends you on a real Kohl's marketing website. At least the Zulu URL Risk Analyzer knows that this email is 100% malicious!

Kohls contact@damagenoiseexposure.com.au
Confirmed: Your Kohls Reward @ no cost!

http://fur.tumultuoustradetensions.com.au/N1B2Q1E6s5OvOOXD-KhDOODDKDO-hhhvK



Unsubscribe Here
2360 Corporate Circle Henderson, NV 89074

If you would like to stop receiving these emails, please Unsubscribe here

zscaler Zulu URL Risk Analyzer

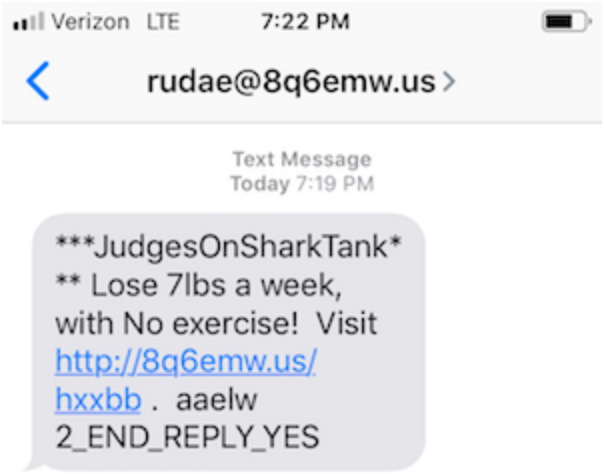
URL Information

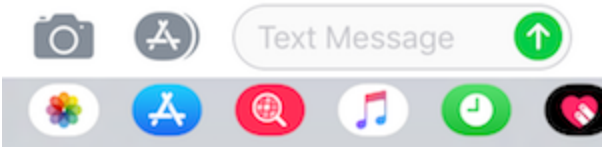
http://fur.tumultuoustradetensions.com.au/N1B2Q1E6s5OvOOXD-KhDOODDKDO-hhhvK

User-Agent
Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko

Test Results
Malicious
100/100

We received this text from the email address **“rudae “@” 8q6emw[.]us”** on October 12 with a link about losing 7 pounds in a week without exercising. Incredible claim, right? The link pointed back to that strange website **8q6emw[.]us**. A WHOIS lookup informs us that this domain was registered by someone named William Weatherall on the same day we received that text. Mr. Weatherall listed his address as 4950 Brownton Road,
Marks, MS, 38646. There’s a small problem with that address. Google Maps cannot find any such road named Brownton in Marks, Mississippi. Does this claim sound trustworthy to you? Sounds much more like a malware threat is waiting for you at the end of that link.





Top Story: Beware of Extreme Claims
During the last few weeks we’ve written about dozens of malicious emails (there have been hundreds!) that are being sent from domains that end with the global top level domain “best.” We’re finding that many of these malicious emails use extreme claims to try to trick recipients into clicking their way to a computer infection. We thought we would focus some attention on these extreme claims to give our readers an idea how cybercriminals try to engineer our behavior.

As you read the opening text in each of these emails, notice how manipulative they are to engage your clicking behavior! The link in each is indicated by the “=>”

FROM: Back Pain Yoga <backpain “@” calibicon[.]best>
Emily was just 12 years old the night she thought she was going to die...
Out in the middle of the pitch black New Mexico desert, suddenly paralyzed and sur-rounded by shattered glass...
...she can still remember counting each breath, wondering if it was going to be her last.
Fighting for her life that night, Emily had no idea her nightmare had only just begun, as the events from that horrific night would come back over 15 years later to nearly destroy her life...
...and that's when something miraculous happened.
Seemingly out of nowhere, Emily stumbled onto this 1 unusual stretch that completely eliminated her back pain and sciatica, and just in time to save herself from dangerous and life-threatening surgery:
=> 1 Weird Stretch HEALS Back Pain and Sciatica.

FROM: Home Solar System <homesolarsystem “@” quezmolt[.]best>
Wall street confirms all share holders are selling hard after this weird cheap solution popped on the radar...
And they have every reason to...
Over 18,000 Patriots are using the system in their homes... (and that's just in the last three months)
They get unlimited energy for less than 80 cents a day... Without paying one nickel more to their electricity provider!
If you're skeptical... => Just watch this short video... and you'll be able to cut your power bills to almost ZERO in just 45 minutes!

FROM: Protective Eyewear <eyehealth “@” artcoriz[.]best>
The glasses company lawyers are doing everything they can to make us take it down...
But this video shows you a secret "Tennis Ball" technique to improve your vision in just 3 days...
==> Here's the link, make sure you watch it while you still can:

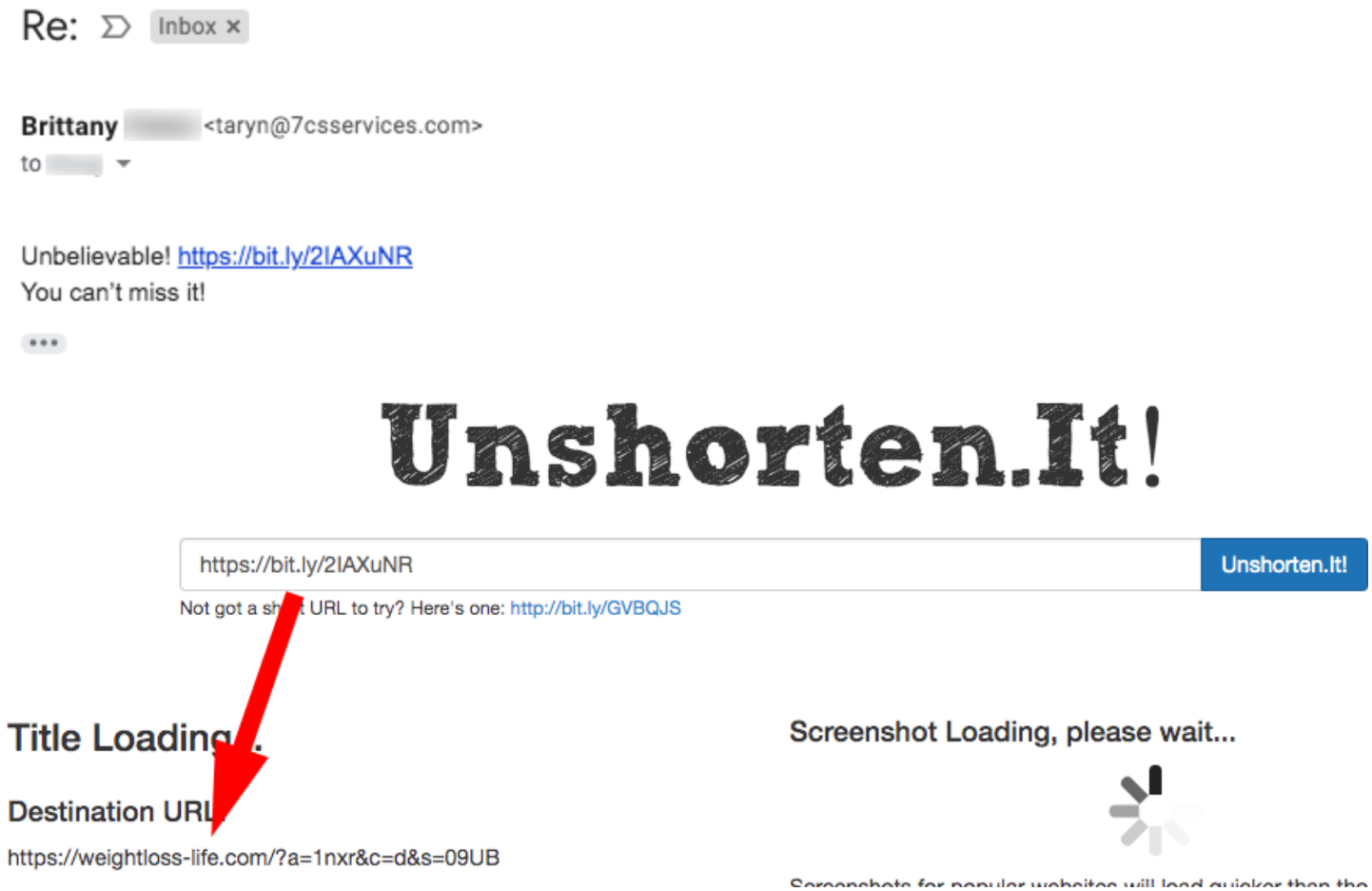
FROM: Science Based Diet <healthfood “@” technet[.]best>
Drinking the "recommended" amount of water every day makes you age FASTER?
It sounds insane, but according to scientists the answer is YES.
And you'll never guess the reason why... (Hint: It's NOT about the purity of your water).
So don't even think about reaching for your next water bottle until you've watched this alarming video.
To be honest, this sounded like complete nonsense to me at first...
But then I saw the science behind this discovery that's already changed minds and the lives of more than 79,000 people...

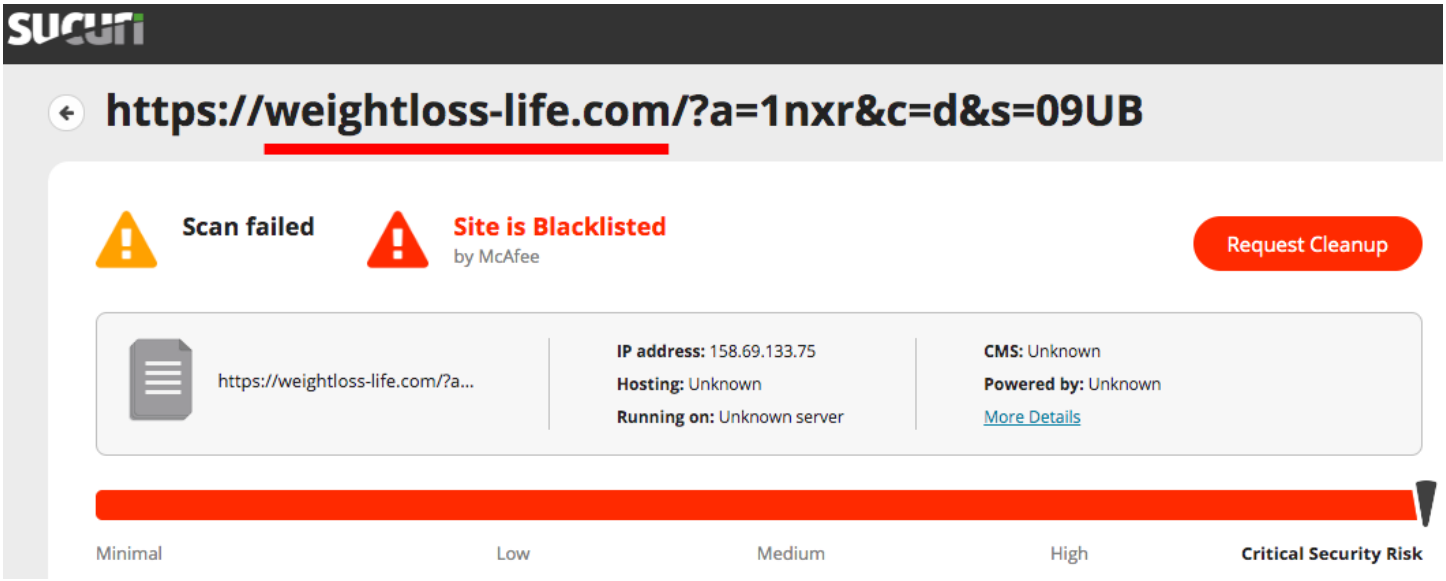
FROM: Improve Your Memory <brainpower “@” protrexonkont[.]best>
If you want to prevent and reverse memory loss and even dementia, you want to add this delicious hot drink on the breakfast table.
The reason why?
Drinking one cup of this every day reduces your risk of developing dementia by 86%, according to studies.
This secret and other memory-boosting tricks are leaked from a secret manuscript locked in the Vatican church. Inside, there was Dracula's royal secret to perfect memory.

There's more: 9 out of 10 people who drank the beverage and then added some tasty ingredients to their meals significantly improved their memory in days.

FROM: Freedom Box Generator <alternativeenergy “@” quinisk[.]best>
A Chinese company created the ultimate computer, capable to do several millions of calculations per second. This was supposed to be used for research, but some people got their hands on these devices and begin making serious money with them.
They have created some huge facilities, making them millions of dollars every month.
Word got out that companies were making untracked money by putting these machines to function and the Chinese Government banned using them on their territory.
Watch this video for the full story on how you could benefit from using these machines in your home. You get both money and free heat by using them, so I would recommend checking it out.

For Your Safety: Unbelievable!
Criminals continue to target people through the hacked email accounts of friends and acquaintances, such as this email. “Unbelievable! …. You can’t miss it!” includes a shortened **bit.ly** link. This shortened link will forward you to a website that looks OK (at **weightloss-life[.]com**) but is already blacklisted and dangerous!





Until next week, surf safely!

info@thedailyscam.com

Free Newsletter Every Wednesday