PROTECTING YOUR PERSONAL DATA

Presented by

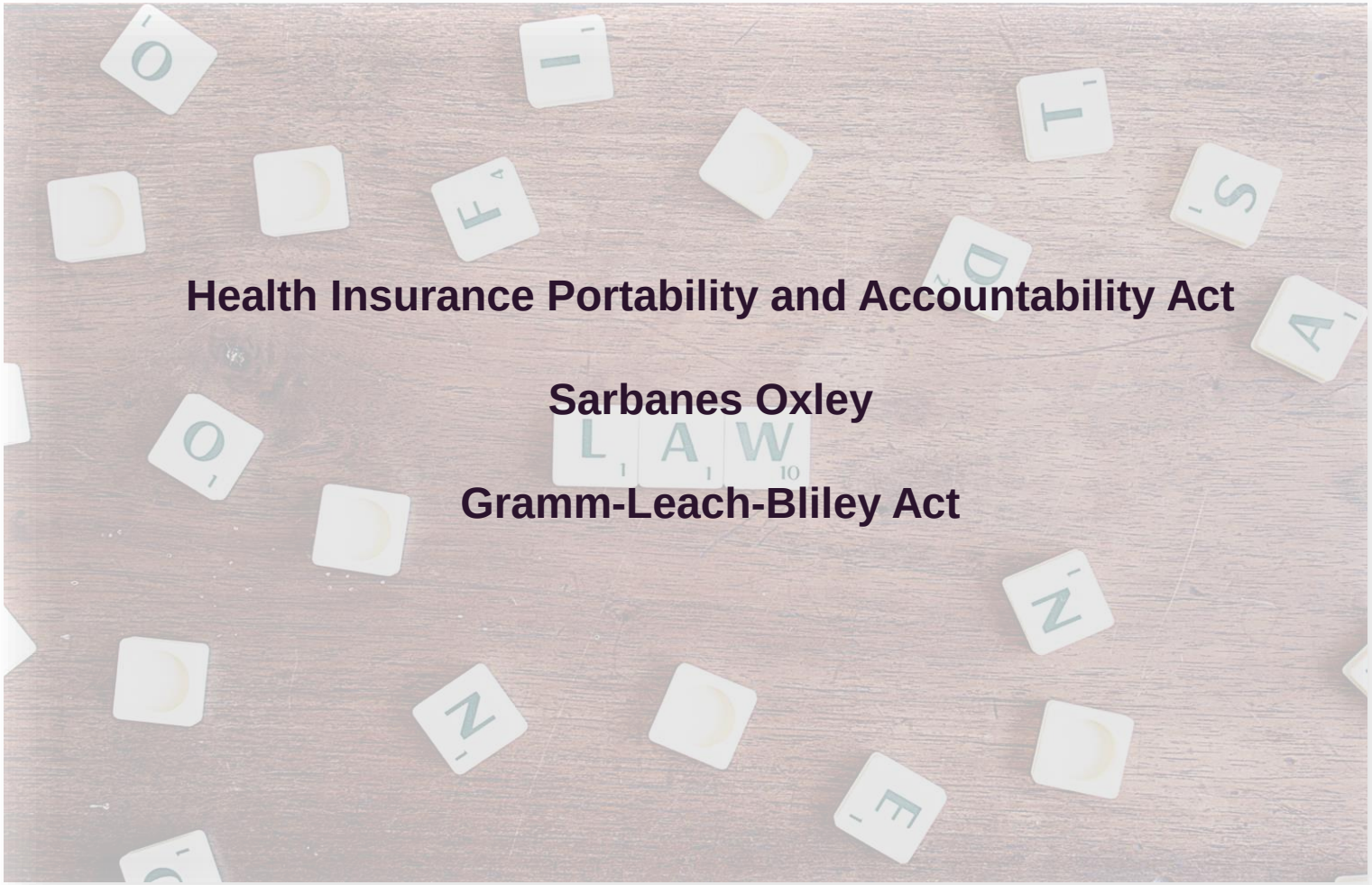
Anne Saita
asaita@twirlingtigermedia.com

Why me?

Why you?

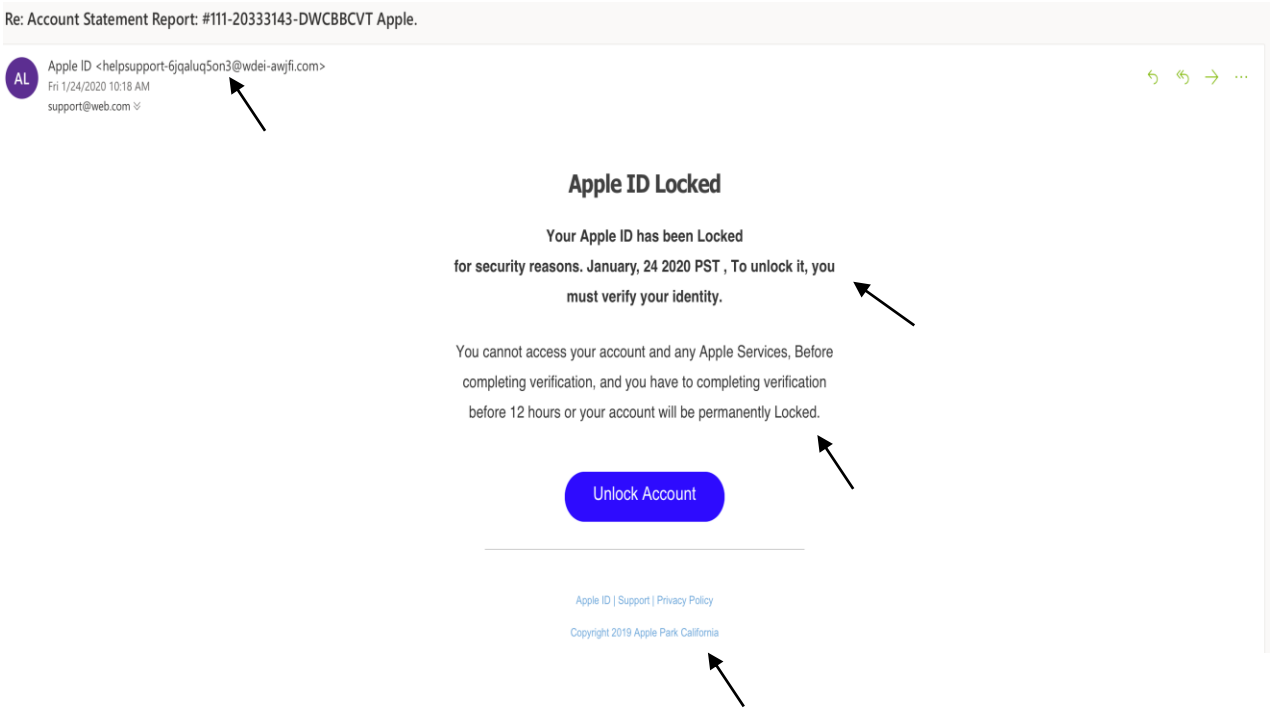
Why you?

Why now?

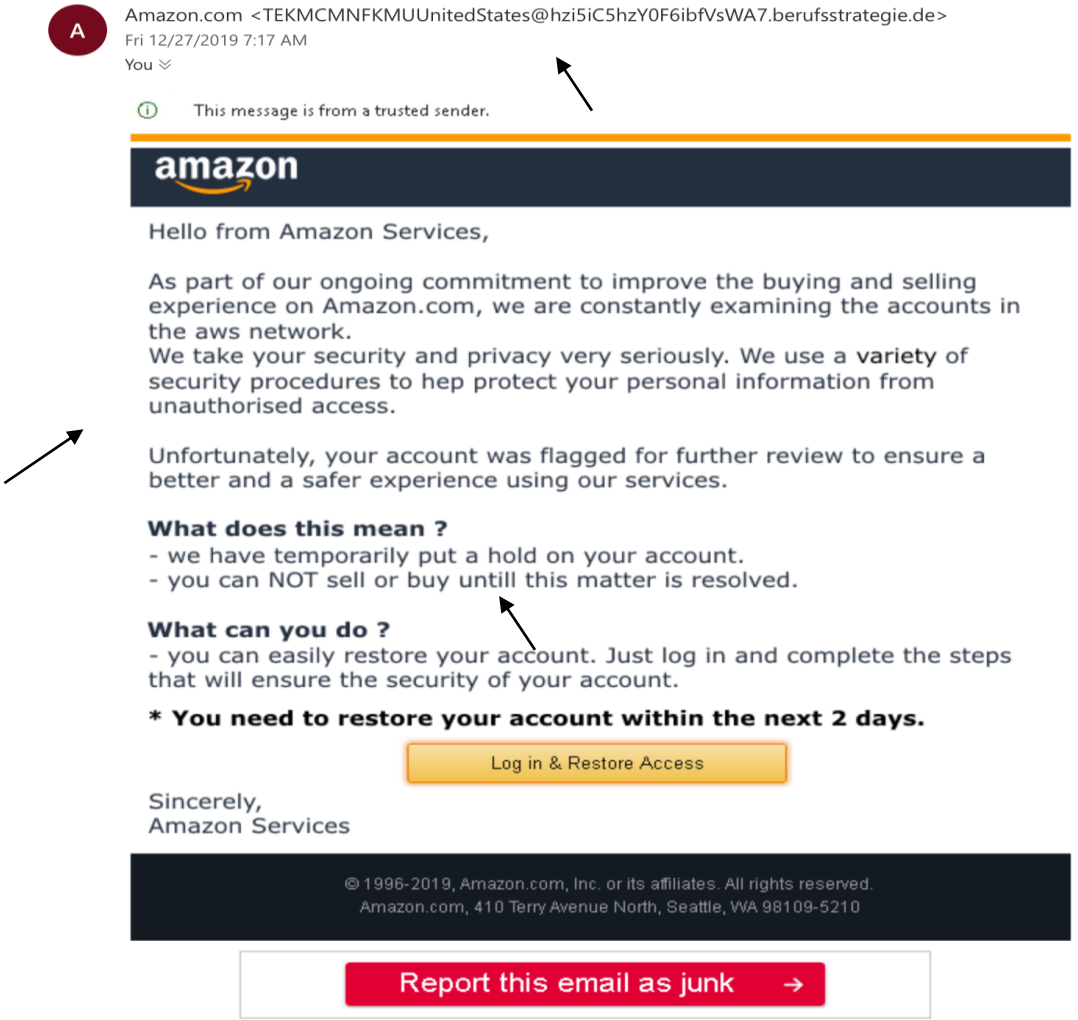


Why now?

Coming to an inbox near you



Coming to an inbox near you



A

Amazon.com <TEKMCMNFKMUUnitedStates@hzi5iC5hzY0F6ibfVsWA7.berufsstrategie.de>

Fri 12/27/2019 7:17 AM

You

This message is from a trusted sender.

amazon

Hello from Amazon Services,

As part of our ongoing commitment to improve the buying and selling experience on Amazon.com, we are constantly examining the accounts in the aws network.
We take your security and privacy very seriously. We use a variety of security procedures to hep protect your personal information from unauthorised access.

Unfortunately, your account was flagged for further review to ensure a better and a safer experience using our services.

What does this mean ?
- we have temporarily put a hold on your account.
- you can NOT sell or buy untill this matter is resolved.

What can you do ?
- you can easily restore your account. Just log in and complete the steps that will ensure the security of your account.

*** You need to restore your account within the next 2 days.**

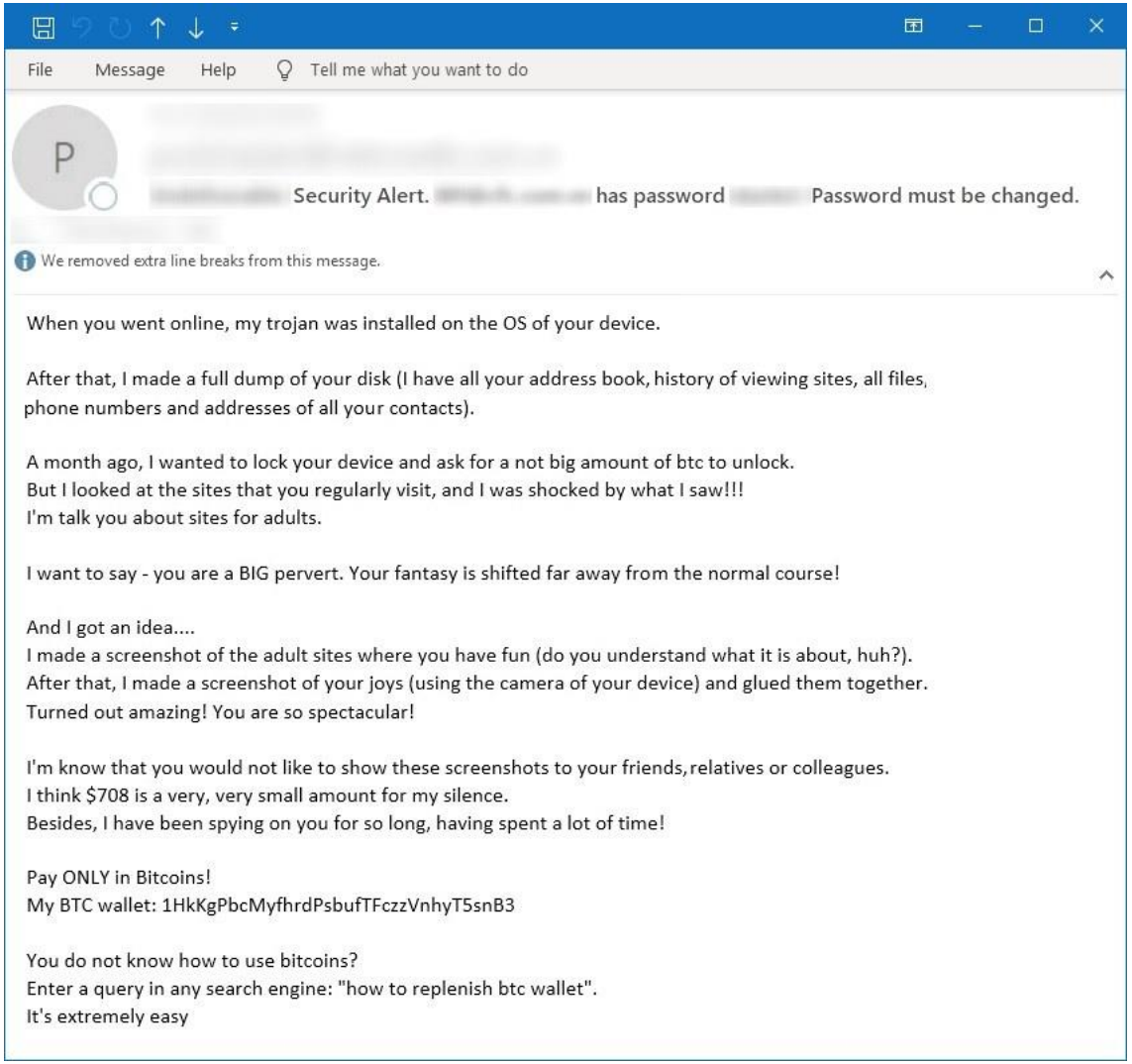
Log in & Restore Access

Sincerely,
Amazon Services

Amazon.com, 410 Terry Avenue North, Seattle, WA 98109-5210

Report this email as junk →

Coming to an inbox near you



File Message Help Tell me what you want to do

P

[redacted] Security Alert. [redacted] has password [redacted] Password must be changed.

We removed extra line breaks from this message.

When you went online, my trojan was installed on the OS of your device.

After that, I made a full dump of your disk (I have all your address book, history of viewing sites, all files, phone numbers and addresses of all your contacts).

A month ago, I wanted to lock your device and ask for a not big amount of btc to unlock.
But I looked at the sites that you regularly visit, and I was shocked by what I saw!!!
I'm talk you about sites for adults.

I want to say - you are a BIG pervert. Your fantasy is shifted far away from the normal course!

And I got an idea....
I made a screenshot of the adult sites where you have fun (do you understand what it is about, huh?).
After that, I made a screenshot of your joys (using the camera of your device) and glued them together.
Turned out amazing! You are so spectacular!

I'm know that you would not like to show these screenshots to your friends, relatives or colleagues.
I think $708 is a very, very small amount for my silence.
Besides, I have been spying on you for so long, having spent a lot of time!

Pay ONLY in Bitcoins!
My BTC wallet: 1HkKgPbcMyfhrdPsbufTFczzVnhyT5snB3

You do not know how to use bitcoins?
Enter a query in any search engine: "how to replenish btc wallet".
It's extremely easy

Coming to an inbox near you

‘Crisis’ communications

Since the global pandemic, cybersecurity vendors are seeing:

- Malware masquerading as legit-looking news reports on the novel coronavirus spread.
- Phishing emails offering much desired COVID-19-related supplies at a discount (masks, medical supplies, paper goods).
- Fraudulent virtual exchanges between “bosses” and “coworkers” asking for sensitive files.
- “Zoombombing”

Insider threat

Third-party risks

Target: An HVAC contractor

Capital One: A cloud service employee

Equifax: An imposter client

This is how easy it still is

What to do

Use strong, unique passwords

- Mix of numbers, letters and characters at least 8 characters long
- A personal word or phrase you can remember that's unique to you

EX: S0l@n@B3@ch

- Multi-factor authentication
- Never reset passwords over public Wi-Fi
- Never share passwords with friends
- Consider a password manager

What to do

Be very, very careful using ‘Free Wi-Fi’

- More than one way to hack (sniff sniff, looky-loos)
- If you use a wireless router, protect it with your own password
- Turn off auto-roam for strongest Wi-Fi signal on your phone, laptop or tablet
- Use a VPN (virtual private network)

What to do

Practice good cyber hygiene and ‘social distancing’

- Install anti-malware software on all mobile and desktop devices—and update it frequently
- Install legitimate software updates, especially if they say they seal security holes. Avoid outdated software and operating systems no longer supported by a vendor.

What to do

Practice good cyber hygiene and 'social distancing'

- Don't click on a link without vetting it, even if it appears from a friend or other trusted source.
- Remove suspicious online comments in your feeds
- Stop trying to be everyone's friend
- Beware of spoofs

What to do

- Tell us about your vacation--after you return.
- Don’t download pictures without knowing their true source.
- Never send sensitive account information over email. Call and speak with a live operator—and test them if something seems “off.”
- Think thrice before giving your full Social Security number on forms. Trust, but verify. And everyone has a substitute number to use instead.

What else?

Watch what you say, even at home

- If you have a virtual personal assistant like Google Home or Alexa, they are always “on” and listening unless you physically unplug them.
- Never, ever talk about sensitive information in their presence.
- Be aware that any smart device (coffee maker, refrigerator, Ring doorbell, etc.) can be hijacked to launch an attack or to attack YOU.

What else?

Use those privacy settings and SSL

Only purchase from sites that begin with https:// (lock symbol)

Check yourself

Periodically check the website https://haveibeenpwned.com to see if you're personal data is out there due to someone else's negligence.

What else?

Most secure web browsers

Trinity College in Dublin most recently researched and ranked the most popular web browsers from best to worst in terms of sending data that could track users over time.

Brave
Chrome
Firefox
Safari
Microsoft Edge
Yandex

And…?

Monitor your credit reports

Every U.S. consumer is entitled to check their own credit reports with the three major agencies (TransUnion, Experian and Equifax) for FREE once every 12 months.

You must use this FTC-approved website: annualcreditreport.com

From 2020-2026, you can access a free report from Equifax SIX times throughout the year. Plus the two freebies from Experian and TransUnion.

Let’s review those tips again

- Use strong, unique passwords that are never shared and are securely stored.
- If you must use public Wi-Fi, scramble your data in transit using encryption (such as a VPN).
- Be careful who you interact with online and what you share and when.
- Use privacy settings for social accounts; anti-malware on ALL devices.
- Regularly monitor for suspicious activity.
- Remember: Alexa can’t help it; she’s programmed to snitch.

OK, your turn.