Sextortion Scams - Know it all

www.thecyphere.com info@thecyphere.com

Phishing vs sextortion scams

www.thecyphere.com info@thecyphere.com

Phishing is when cyber criminals try to steal your confidential information through "seemingly-legit" messages or emails.

Sextortion scams are a type of phishing attack where cyber criminals try to **blackmail** you, claiming they have a video of you visiting adult sites and they threaten to disclose it unless you pay a ransom (usually in BitCoin).

These baddies asking for ransom

don't really know if you have used your webcam (or even have one!) or ***visited adult sites***. They're just trying to work on your fear factor into paying the ransom.

Millions of such emails are sent in the hope that victims will pay. Some tricks that are used to make such emails convincing are included in the upcoming slides.

How To Identify Sextortion Scams?

(Includes a sample sextortion email)

www.thecyphere.com info@thecyphere.com

Ask search engines first

- Based on the certain words/phrases or contents of the email (exclude **your** details), check search results for any forum results, entries of such content as spam, blacklisted domains or other artefacts.

Unusual Sender Details

- Be cautious of unfamiliar or suspicious email addresses.
- Check the sender's domain for misspellings or slight variations.
- Legitimate organisations will use official domains for communication.

Urgent Language & Threats

- Scammers often create a sense of urgency or fear to manipulate victims.
- Stay vigilant of subject lines or content that demand immediate action or threaten negative consequences.

Generic Greetings & Poor Grammar

- Scam emails often use generic greetings like "Dear Customer" instead of your name, or sometimes don't use any greetings.

- Watch out for grammar and spelling errors and strange words in the email content.

Suspicious Links & Attachments

- Avoid downloading attachments or clicking on links from unknown sources.
- Hover over links to preview the URL – ensure they lead to legitimate websites.

Includes your leaked info

- Sometimes cybercriminals include your leaked password to make the email look legit to add to the urgency of the situation and fear factor.

Demands for Money

- Threats to expose your sensitive content
- Demands for payment in cryptocurrency to avoid detection
- Urgency in email language for quick ransom payment to prevent embarrassment

Sextortion emails rose by **178%** from 2022 to now, becoming a major email threat. ESET reported them as the third-highest email threat in H1 2023.

Source: Infosecurity Magazine

Greetings!

A sample sextortion scam email highlighting various factors i.e. red flags, indicators.

I have to share bad news with you. Approximately a few months ago, I gained access to your devices, which you use for internet bro[redacted] started tracking your internet activities.

Here is the sequence of events:

Some time ago, I purchased access to email accounts from hackers (nowadays, it is quite simple to buy it online). I have easily managed to log in to your email account[redacted]

Includes your email address here

One week later, I have already installed the Cobalt Strike "Beacon" on the Operating Systems of all the devices you use to access your email. It was not hard at all (since you were following the links from your inbox emails). All ingenious is simple. :).

a persistent connection established with your system

This software provides me with access to all your devices controllers (e.g., your microphone, video camera, and keyboard).
I have downloaded all your information, data, photos, videos, documents, files, web browsing history to my servers. I have access to all your messengers, social networks, emails, chat history, and contacts list.

My virus continuously refreshes the signatures (it is driver-based) and hence remains invisible for antivirus software. Likewise, I guess by now you understand why I have stayed undetected until this letter.

persuasion factor to connect the dots on how access was achieved

While gathering information about you, i have discovered that you are a big fan of adult websites. You love visiting porn websites and watching exciting videos while enduring an enormous amount of pleasure. Well, i have managed to record a number of your dirty scenes and montaged a few videos, which show how you[redacted]ms.

If you have doubts, I can make a few clicks of my mouse, and all your videos will be shared with your friends, colleagues, and relatives. Considering the specificity of the videos you like to watch (you perfectly know what I mean), it will cause a real catastrophe for you.

Threat

I also have no issue at all with making them available for public access (leaked and exposed all data).
General Data Protection Regulation (GDPR): Under the rules of the law, you face a heavy fine or arrest.
I guess you don't want that to happen.

As an individual this isn't applicable to you - just a buzzword thrown in to strengthen his/her case

Let's settle it this way:

You transfer $1857 USD to me and once the transfer is received, I will delete all this dirty stuff right away. After that, we will forget about each other. I also promise to deactivate and delete all the harmful software from your devices. Trust me. I keep my word.

the ransom

That is a fair deal, and the price is relatively low, considering that I have been checking out your profile and traffic for some time by now. If you don't know how to purchase and transfer Bitcoin - you can use any modern search engine.

You need to send that amount here Bitcoin wallet:
bc1qm0m3qlcacj4recwd2dtycl9gweqdvxp5z8e6sk

ransom deposit wallet address

(The price is not negotiable).
You have 2 days in order to make the payment from the moment you opened this email.

Do not try to find and destroy my virus! (All your data is already uploaded to a remote server).

Threats

Do not try to contact me. Various security services will not help you; formatting a disk or destroying a device will not help either, since your data is already on a remote server.

This is an APT Hacking Group. Don't be mad at me, everyone has their own work.
I will monitor your every move until I get paid.
If you keep your end of the agreement, you won't hear from me ever again.

How To Protect Yourself Against Sextortion Scams?

www.thecyphere.com info@thecyphere.com

Secure Your Online Presence

- Use strong and unique passwords for all accounts.
- Implement Multi-Factor Authentication (MFA).
- Regularly update your passwords and avoid using guessable information.

Educate Yourself & Others Around You

- Stay informed about the latest scams and phishing techniques.
- Educate friends and family about the risks of sextortion phishing.

Verify Requests & Contacts

- Before taking any action, independently verify requests through official channels.
- Double-check email addresses and website URLs for authenticity.
- Don't share personal information without confirming the legitimacy of the request.

Boost Your Privacy Settings

- Review and adjust your social media privacy settings.
- Refrain from sharing personal information publicly online.
- Restrict access to your online profiles to trusted individuals.

Report & Block Suspicious Messages Or Emails

- Report phishing emails to your email provider or relevant authorities.
- Block and filter suspicious email addresses to prevent further contact.

What To Do If You Have Received A Threatening Email?

www.thecyphere.com

info@thecyphere.com

Do Not Communicate With The Email Sender

- Don't engage with the cybercriminals.
- If you're unsure about the email, send it report@phishing.gov.uk and delete it.

Should I pay the ransom?

- That’s what cybercriminals are looking for. Do not pay the ransom.

Check your leaked passwords

- Don't worry if your password is disclosed; it might be from a past data breach. Check it here: https://haveibeenpwned.com/

Change Your Passwords

- If your current password is listed, change it right away and never use easily guessable passwords or your personal information in your passwords.
- NOW is the time to start using a password manager.

In case you paid the ransom already

- Contact Action Fraud for further advice (www.actionfraud.police.uk).

LIKE THIS?

- [ ] Share  with others
- [ ] Follow for similar content in the future

www.thecyphere.com **info@thecyphere.com**