SEXTORTION EMAILS...

Phishing Emails that Use Fear and Shame as a Weapon

The Problem Is Growing.

Cofense Labs has been monitoring the largest confirmed dump of email addresses used for sextortion to date. The stats below are based on an analysis from January 1, 2019 - June 30, 2019.

330,000,000+

Number of Unique Compromised Accounts

7,854,099

Number of Sextortion Emails Cofense Labs Has Analyzed

How Does Sextortion Work?

Typically, sextortion emails claim to have taken control of your webcam and filmed you in a compromising situation. Other times the email might threaten to reveal browsing history on adult sites.

Attackers Want Payment in Bitcoin.

To add credibility, the email will often include Personally Identifiable Information (PII) like your username or an old password. Payment is requested (usually via Bitcoin) and the scammer threatens to send the video to your contacts unless you pay up.

- **17,090**: Number of Bitcoin Wallets Identified across Analyzed Emails
- **1,265**: Total Transactions (Victims)
- **155.907840**: Total Bitcoin Paid
- **$1.8M**: Total Approximate Dollar Value of Payments

Tips to Handle and Avoid Sextortion...

Education is the best defense. Here are some things to know.

How did the scammer know your information?

Many popular sites you use every day have encountered a data breach. Data breaches publicize PII like usernames, passwords, addresses, and other sensitive information.

Extortionists use these breach repositories to find material, then craft convincing phishing emails. They often use an automated script to send out thousands of personalized emails.

If you receive one of these phishing emails:

We Recommend You DON'T Respond.
Replying verifies to the scammers that they have found a valid email address and this may make you a target in future phishing attacks.

We Recommend You DON'T Pay.
It's almost impossible to track cryptocurrency transactions or recover funds. Paying with a credit card or PayPal account is not any safer and may result in further compromises and charges.

We Recommend You DON'T Engage.
Typically, sextortion emails do not have common phishing elements - a link or attachment. If however, they do include these - don't click on links or attachments.

Remember:

Don't use the same password across different sites.
Attackers will use passwords found on one breached site to launch attacks on others.

Use complex passwords and change them regularly.
A password manager application can help you securely manage credentials and can quickly generate complex passwords. When you're able, create a unique login for each website, with a unique password.

Think Twice.
Read emails thoroughly and be wary of emails that use emotional triggers like fear, embarrassment, or threats.

Use a cover on your webcam when not in use.
Purchase a cover that clips on or slides closed when you're not using the camera. If they can't see you - they can't threaten as if they can!

Some additional helpful tips:

Restrict access to online profiles. Set limits on who can view your profile.

Keep your private information private. Avoid revealing sensitive information in public forums.

Be suspicious. Don't take any information you receive from a new online contact at face value. Be smart and protect yourself.

Only use your corporate email address for business purposes, especially with social media accounts like LinkedIn.

If you suspect that you have received a sextortion email at work, report it immediately!

See if your business is exposed to sextortion: https://cofense.com/sextortion

COFENSE