SEXTORTION EMAILS

PHISHING EMAILS THAT USE FEAR & SHAME AS A WEAPON

Sextortion is a cybercrime that occurs when organised criminals and predators threaten to expose a sexual image / video, or pornography usage often stolen from a computer / mobile or by hacking into a webcam to blackmail for money, or force victims to engage in some form of sexual activity. Offenders target multiple victims, a majority of whom are children under the age of 18.

THE PROBLEM IS GROWING

330,000,000+

Number of Unique Compromised Accounts

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*

Data source: *Cofense Labs*

7,854,099

Number of Sextortion Emails Analysed

Data source: *Cofense Labs*

HOW ARE VICTIMS TARGETED ?

SOCIAL MEDIA MANIPULATION IS USED IN **91%** OF CASES INVOLVING YOUNG VICTIMS

COMPUTER HACKING IS USED IN **43%** OF CASES INVOLVING ADULT VICTIMS

WHO ARE THE VICTIMS ?

71 % of cases involve victims under the age of 18.

14% of cases involve a mix of young and adult victims.

12% of cases involve adult victims.

WHO ARE THE PERPETRATORS ?

EVERY PROSECUTED PERPETRATOR IS MALE

They include college students, friends, and family of the victim.

SEXTORTIONISTS TEND TO BE PROLIFIC REPEAT OFFENDERS

Among the cases studied:

25 cases involved at least	13 cases involved at least	13 cases involved more than
10 VICTIMS	20 VICTIMS	100 VICTIMS

HOW SEXTORTION WORKS?

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.

17,090

Number of Bitcoin wallets identified across analysed emails

1,265

Total transactions (Victims)

155.907840

Total Bitcoin Paid

$1.8 million

Dollars paid by victims

CRIMINALS 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 (Usally via Bitcoin) and the scammer threatens to send the video to your contacts unless you pay up.

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 vary 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. It they can't see you, you know the threat is false.

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.

FOR ADULTS ONLY USE WORK EMAIL ADDRESS FOR WORK PURPOSES.
Especially with platforms like Linkedin.

IF YOU SUSPECT THAT YOU HAVE RECEIVED A SEXTORTION EMAIL AT WORK, REPORT IT IMMEDIATELY!

CALL FOR INFORMATION, ADVICE OR IF YOU JUST WANT TO TALK

Prevented
ABUSE PREVENTION EDUCATION

IF YOU SUSPECT ABUSE CALL NSPCC HELPLINE
0800 800 5000

IF YOU'RE A CHILD & WANT HELP CALL CHILDLINE
0800 1111

NNECA
NATIONAL NETWORK TO END CHILD ABUSE
WWW.NNECA.ORG.UK
WWW.CHILDABUSEHELP.ORG.UK