INTERPOL

CONNECTING POLICE FOR A SAFER WORLD

Sextortion – Questions and Answers

1 HOW COMMON IS SEXTORTION?

Given the nature of the crime, and to avoid potential embarrassment, many victims do not come forward, so it is difficult to provide figures. However, reports indicate that this is a growing problem with hundreds of thousands of victims across the world.

Continued expansion of Internet access, especially in developing countries, is likely to produce an even larger pool of potential victims in the future.

2 HOW ARE THE VICTIMS TARGETED?

Individuals may be targeted through any number of different websites, including social networking, dating, webcam or adult pornography sites. In some cases, victims have been identified via pornography sites where they entered their credit card details. There is no one specific method or social network used. The single common factor in all cases is for the organized crime group to make money.

Resourceful and practiced criminals target hundreds of individuals around the world with the so-called 'scatter shot' approach aimed at increasing their chances of finding a victim.

3 WHAT ARE THE STEPS INVOLVED?

The organized crime groups involved in this type of crime are very sophisticated and recruit 'agents', often providing monthly incentives for the best-performing blackmailer.

An example of sextortion is where the agent/blackmailer will assume the identity of an attractive man or woman to engage a victim. After gaining their trust, the agent will record footage of the victim performing a sexual act, which they threaten to circulate amongst the victim's friends or post on the Internet unless an amount of money is paid, typically ranging from USD 500 to USD 15,000.

In another method, the engagement between the victim and the criminal is interrupted on the criminal's side by a child appearing on screen during the sex act. All contact is then cut. A demand follows, often on police headed paper telling the victim that unless they pay, a police investigation will be started. The police will NEVER contact anyone in this way. It is obvious extortion.

4 WHAT SHOULD SOMEONE DO IF THEY BELIEVE THEY ARE BEING TARGETED?

Anyone who believes they are being targeted should immediately cease all contact with the individual and report the matter to their local police and online service provider. If it is via a social network, the administrator should also be alerted. Do not pay the money that is being demanded. Remember that this is organized crime. You are not the only one to fall for these scams but you can help to stop them by reporting it as quickly as possible and by refusing to pay. If you are a child please talk to a trusted adult. It may seem there is no way out, but there are people who can help.

5 WHY ARE ORGANIZED CRIME GROUPS INVOLVED?

Organized crime networks are involved in sextortion as it involves little investment and low risk for comparatively high financial gain. Victims usually feel trapped by circumstance and are reluctant to report it to the police. The Internet also allows for a large number of people to be reached with comparative ease.

6 HOW MUCH MONEY IS MADE THROUGH THIS TYPE OF CRIME?

The average blackmail demand is USD 500, however demands of up to USD 15,000 have been reported. It is not possible to put an exact amount on profits being generated by organized crime, however it certainly runs to tens of millions of dollars. The demands are kept low as these represent amounts that the average person might have access to and would make them less likely to report it to the police. Although the demands can be considered low for an adult, these can appear an enormous amount of money if the victim is a child.

7 WHICH SOCIAL NETWORKS HAVE THE MOST SEXTORTION VICTIMS?

Any and all social networks can be abused to target victims. The environment in which fraud or extortion of this nature can take place is created and built on communication. Social networks and all other means of communication facilitate that.

8 WHAT ARE SOCIAL NETWORKS DOING TO PREVENT THESE CRIMES?

Private sector companies support the law enforcement community in helping to identify those responsible and to protect members of the public from potential abuse. As in most fraud cases, the exchanges which take place between the victim and the offender are indistinguishable from normal social networking. This creates a challenge for everyone concerned including the victims. It is important to remember that this type of extortion and fraud existed a long time before the Internet or smartphones but they are facilitated by today's connectivity and the ease of communication.

It is important for users to report this type of crime promptly so that social networking sites can investigate quickly and pass on the information to the police. Speed is vital as the data gathered online, such as the IP address of the computer used, is time-sensitive.

For information about specific prevention activities, please contact the social networks directly.

9 WHICH COUNTRIES ARE AFFECTED IN PARTICULAR?

To date, the majority of countries where victims have been targeted are those where English is a primary Internet language, such as the UK, USA, Australia, Singapore, Hong Kong, Indonesia and Malaysia. Criminal gangs will generally operate between countries with a common language. We are seeing similar crimes emerging in French-speaking Africa, targeting France.

10 HOW MANY SEXTORTION VICTIMS HAVE TAKEN THEIR OWN LIVES?

Whilst there are reports from around the world of victims having committed suicide or seriously self-harmed after becoming victims of sextortion, there are no exact figures. Victims of this type of fraud and cruel emotional manipulation can be affected in many different ways. Please seek help if you are experiencing this type of crime. It is easily dealt with and the damage can be minimized by getting trusted friends, counsellors or adults involved.