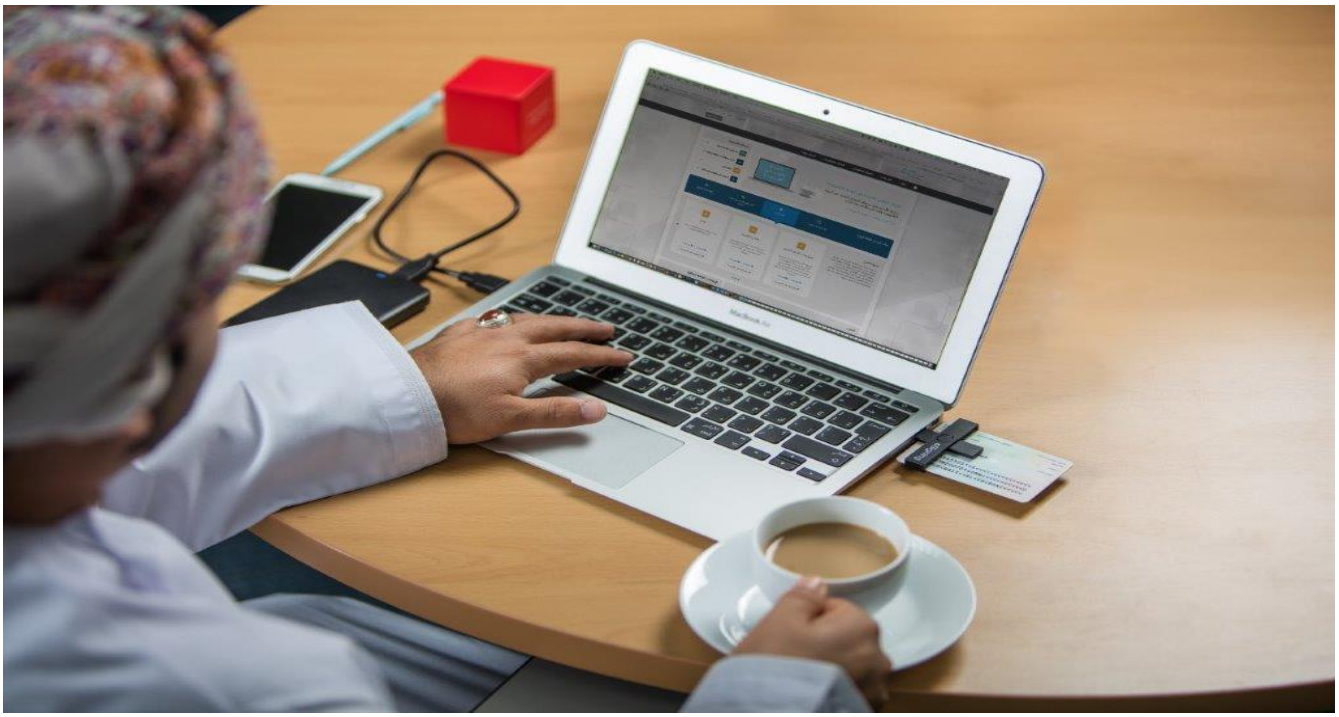
More than 269 cases received since 2011 and Oman CERT warns of Blackmail incidents

- **Most of the cases that are reported and dealt with target people aged 18 to 50 years**
- **The percentage of men cases is approximately 90%, as females usually don't report this type of cases**
- **More than 161 blackmail cases received from Jan 2016 until today**
- **Percentage of cyber blackmail cases compared to all cybersecurity cases handled by the center this year is 45.35%**

What is blackmail?

The Omani law defines blackmail as threatening someone to compel a person to do any act or wrong doing against his/her will, with some form of punishment if he/she does not fulfill the request. As for penalties, the cybercrime law identified in the eighteenth article a period not less than one month and not more than three years and a fine of not less than one thousand RO and not more than three thousand RO or one of these penalties. The penalty shall be temporary imprisonment for not less than three years nor more than ten years and a fine of not less than three thousand RO and not exceeding ten thousand RO if the threat to commit a crime or breach of the attribution of moral turpitude.



[Grab your reader's attention with a great quote from the document or use this space to emphasize a key point. To place this text box anywhere on the page, just drag it.]

Cyber blackmail in Oman

Eng. Bader Al Salehi, Director General of Oman CERT, warned of the increasing number of cyber blackmailing cases received through Oman National CERT. He said: "Since 2011 we received 269 blackmailing cases and of which 161 cases only this year!"

Al Salehi also added: "cyber Blackmail issue is not limited to a country without the other, and although the Sultanate is ranked 1st in the global cyber-security index among Arab countries and 3rd worldwide, the number of blackmail cases are increasing and affecting everyone, including employees working in critical places in the state, not to mention the cases of young men and women faced on a daily basis and on an alarming forms which sometimes may cause them to commit suicide."

On the motives behind cyber blackmail, Al Salehi said: "Based on the cases that we receive at the OCERT, there are two main motives: the first is the financial blackmail in which the blackmailer requests money for the disclosure or dissemination of personal information and this kind mostly targets males, while the second type is sexual blackmail that targets females and it is a type of sexual harassment, whether verbal or physical."

When asked about the countries that such blackmail operations come from, Al Salehi said: "We cannot refer to specific countries from which these attacks come, due to the use of modern techniques of hiding Internet protocols addresses or penetrating other devices through which to blackmail the victims, making it difficult to track the actual location of the blackmailer. The blackmail threat exceeded the normal actions to having an organized groups targeting different segments, and that's what drew the attention of the governments in many countries of the world including the Sultanate to coordinate and cooperate with other countries in the cybersecurity field to address these attacks."

Digital Forensics Lab

This year the Information Technology Authority launched the Digital Forensics Lab in cooperation with the law enforcement organizations in Oman to interpret and analyze electronic data to ensure and help detect cybercrimes and provide courts with the accurate evidence.

[Grab your reader's attention with a great quote from the document or use this space to emphasize a key point. To place this text box anywhere on the page, just drag it.]

What to do when being blackmailed?

On how to act when being blackmailed, Aziza Al Rashdi, Director of Cyber Security Professional Services at OCERT, said: "Prevention is better than cure and we always recommend people to educate themselves on cyber security issues to prevent them from getting any such problems, but if anyone is being blackmailed, we advise them to quickly report to the concerned authorities, including the Royal Oman Police, the Public Prosecution or the OCERT at Information Technology Authority. The victim is advised not to communicate with the blackmailer even when exposed to extreme pressures and not to transfer any money or disclose bank card numbers. Moreover, we advise the victim to avoid any argument with the blackmailer and not to threaten him/her with the police; however, they have to retain all messages or any type of communication to be used as an evidence later on."

[Grab your reader's attention with a great quote from the document or use this space to emphasize a key point. To place this text box anywhere on the page, just drag it.]

Cyber Crime Law

Even when you have been subject to blackmail from outside the Sultanate, you can get your right as the cybercrime law has addressed this issue in Article II: "The provisions of this law shall apply to the cybercrimes, even if committed wholly or partially out of the Sultanate whenever damage to its interests is ensued, or if the criminal result is ascertained within its territories or being intended to be ascertained therein even though not yet ascertained."

With regard to the prosecution of the blackmailer who was outside the Sultanate, Dr. Hussain Al Ghafri, Legal Consultant, said: " This is governed by international and bilateral agreements between the countries, particularly those relating to the extradition of criminals and therefore we can say that: If the blackmailing case occurred from someone outside the Sultanate, and if the Sultanate has an extradition agreement with this country and there is exchange policy between then the blackmailer will be asked for court with the means and procedures set forth in the agreements and diplomatic ways."

[Grab your reader's attention with a great quote from the document or use this space to emphasize a key point. To place this text box anywhere on the page, just drag it.]

Cyber Blackmail effects on society

Hassan bin Ali Al Ajmi, a specialized person in information security and owner of Isnad Company, has warned of the consequences of the increasing number of blackmail cases in the Sultanate. He said: "The situation is very critical and blackmailing is affecting our society, either because of negative attitude and ignorance in using the information and communication technologies or because of recklessness and lack of religious and moral deterrence with a lot of young people. Effects of blackmail touch all age groups of young men and women and children, and even the elderly and some well-known people who work in critical organizations in the country."

In his company, Hassan receives many blackmail cases asking for his help: "This year we received more than 300 blackmail cases and 80% of which are males' cases and 20% females. I believe that ITA is responsible for providing awareness on the use of information and communication technologies then comes the role of ROP, Public Prosecution, the school and the family as a complementary role.

[Grab your reader's attention with a great quote from the document or use this space to emphasize a key point. To place this text box anywhere on the page, just drag it.]

Blackmail in Psychotherapy

Dr. Amal Ambusaidi, Acting Consultant-Psychiatrist -Mood and Anxiety at SQU Hospital, gives some advices on how to deal when being blackmailed: "The effects of blackmailing are beyond being psychologically shocking, but also that what deepens the impact on the individual is feeling embarrassed to seek help and sometimes his/her ignorance of the existence of the support. Therefore, the treatment starts first with dealing with the psychological symptoms suffered by the blackmailing victims seriously and take them out of their isolation."

She elaborated more: "The fundamentals of psychotherapy treatment in general is to treat the patients confidentially, show respect to them, understand their symptoms, gain their trust and provide support and assistance professionally especially those suffering from psychological trauma resulting from physical or psychological abuse. My advice to those who suffer in silence from blackmailing should not hesitate to seek assistance from the concerned authorities which will deal with it professionally and confidentiality and to seek advice and support from a specialist in psychotherapy or psychiatrist for evaluation and guidance for ways to adaption and treatment if necessary."

OCERT Hotline

To report any blackmail cases or any other cyber security incidents, you can contact the Oman CERT through the hotline number: 24166828 or the email: cert999@ita.gov.om during the office hours from 7:30 am to 14:30. Also you can report through the center website www.cert.gov.om

Statistics to be used for an infographic:

1. Number of cyber blackmail cases from 2011 to 2016:

Year	Cyber Blackmail Cases
2011	1
2012	1
2013	5
2014	17
2015	84
2016	161
Total	269

2. The percentage of cyber blackmail cases in terms of gender:

Male	10%
Female	90%

3. The number of blackmail cases compared to the overall cybersecurity crimes in 2016:

No. of cyber blackmail cases	161
No. of cybersecurity crimes	355


عمان الرقمية
e.oman