

# WASPADA Pemeras Ugut SIBER

SUMBANGAN: MAJALAH PC  
SUMBER: CYBERSECURITY MALAYSIA

Penjenayah sering menggunakan taktik menggoda yang berbau seksual (*firts*) untuk menjerat mangsa.

Jenayah peras ugut siber di Malaysia dilaporkan meningkat 18.5 kali ganda pada tahun 2013. Oleh itu, CyberSecurity Malaysia (CSM) mengingatkan orang ramai supaya berwaspada dengan *cyber firts* yang menjurus kepada jenayah peras ugut.

Menurut Ketua Pegawai Eksekutif (CEO) CSM, Dr. Amirudin Abdul Wahab, hanya empat kes peras ugut siber dilaporkan kepada Cyber999 pada tahun 2012 berbanding 73 kes pada tahun 2013. "Peningkatan yang besar dalam insiden peras ugut siber membimbangkan CSM. Kami percaya terdapat lebih banyak kes seumpamanya yang tidak dilaporkan kepada kami. Oleh itu, kami telah mengeluarkan amaran pada 25 Disember 2013 untuk mengingatkan orang awam," jelas beliau.

Mangsa kebanyakannya ialah remaja lelaki sehinggalah lelaki pertengahan umur. Pelaku pula disyaki warga asing, berkemungkinan besar ialah lelaki bersama rakan sekongkol wanita yang mewujudkan hab penipuan di pelbagai lokasi termasuk Malaysia. Kumpulan ini menggunakan rangkaian laman sosial seperti Facebook, Tagged dan sembang video secara *online* seperti Skype sebagai platform untuk menjalankan aktiviti mereka.

## MODUS OPERANDI

Berdasarkan analisis ke atas kira-kira 80 kes yang dilaporkan, CSM mendapati corak modus operandi peras ugut yang hampir sama. Pelaku biasanya

akan membuat profil di Facebook atau Tagged, menggambarkan dirinya sebagai wanita cantik dan seksi yang kononnya berasal daripada Filipina, Jepun atau Korea. Kemudian, wanita ini akan mengenal pasti lelaki yang berpotensi sebagai mangsa dan cuba berbaik-baik dengannya. Wanita itu kemudiannya akan memujuk mangsa untuk melakukan sembang video yang intim.

Semasa sembang video, wanita tersebut akan menanggalkan pakaian dan meminta mangsa melakukan perbuatan yang tidak menyenangkan dan merakam aksi mangsa secara diam-diam. Video rakaman tersebut akan digunakan untuk memeras ugut mangsa supaya membayar jumlah tertentu melalui Western Union atau akaun bank pihak ketiga sekiranya tidak mahu rakaman tersebut diedarkan di media sosial.

## CARA PENCEGAHAN

Bagi mengelakkan diri daripada menjadi mangsa, CSM menasihati pengguna internet supaya berhati-hati dengan segala aktiviti mereka dalam talian, termasuk panggilan video dan suara yang boleh dirakam dan dimanipulasikan. Selain itu, pengguna juga perlu berhati-hati dengan siapa mereka berkawan dan berwaspada dengan aktiviti dalam talian yang mencurigakan.

Mengamalkan amalan terbaik dan etika agama atau sosial semasa berada dalam talian juga boleh membendung pengguna daripada menjadi mangsa. Sebagai langkah pencegahan, pengguna

juga boleh 'mengkonfigurasikan' Skype untuk menyekat komunikasi hanya untuk senarai kenalan sahaja. Gunakan perisian keselamatan yang dikemas kini dan jangan menggunakan kamera web untuk membuat panggilan video kepada orang yang tidak dikenali.

## ATASI PERAS UGUT

Sekiranya anda telah terjerat dan diperas ugut, anda dinasihatkan supaya:

- Hentikan dan elakkan diri daripada terus berkomunikasi dengan pemeras ugut. Abaikan semua panggilan, SMS atau mesej daripada pelaku.
- Keluarkan pelaku daripada senarai kenalan media sosial anda atau letakkan pelaku dalam senarai dihalaang (*blocked list*).
- Privasi semua akaun rangkaian sosial anda supaya pelaku tidak dapat menghubungi anda dan rakan-rakan anda.
- Simpan semua data yang berkaitan seperti log chat, screenshot dan e-mel sebagai bukti bagi tujuan laporan dan pendakwaan.
- Jangan membuat bayaran kepada pemeras ugut kerana ia hanya akan memburukkan keadaan.
- Buat laporan di balai polis berhampiran bersama bukti untuk siasatan lanjut.
- Laporkan ke Pusat Bantuan Cyber999 untuk bantuan lanjut SDK

Tapak web: [www.cybersecurity.my](http://www.cybersecurity.my) atau [www.mycert.org.my](http://www.mycert.org.my)  
E-mel: [Cyber999@cybersecurity.my](mailto:Cyber999@cybersecurity.my)  
Telefon: 1-300-88-2999 (waktu pejabat) atau +6019-266 5850 (24 jam - Kecemasan)