DIGITAL FOR LIFE

Kekal Selamat Dalam Talian

4 penipuan umum

Penipuan Memancing Data berkaitan Perbankan

- Penipu berpura-pura menjadi wakil bank;
- Meminta nama pengguna perbankan internet, Nombor Pengenalan Peribadi (PIN) dan OTP anda.

Contoh mesej penipuan:

> Transaksi akaun 'bank' anda **telah digantung**, sila kemas kini pada 28 Disember atau akaun ini akan dikunci. Sila akses **bit.ly/abc123**

Penipuan Pinjaman Wang

- Penipu menyamar menjadi kakitangan daripada peminjam wang berlesen;
- Kebiasaannya teks SMS atau mesej WhatsApp akan dihantar untuk menawarkan perkhidmatan pinjaman wang.

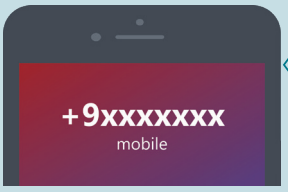
Contoh mesej penipuan:

> PROMO Pelan Ansuran Bulanan:
> 8.88-10.88% (Perniagaan)
> 6.88-8.88% (Peribadi)
> $5-300K Pinjaman sehingga 60 bulan
> tiada kadar tersembunyi
> **SMS/WSAPP ke xxx1231**

Penipuan sokongan teknologi

- Penipu menyamar sebagai pekerja dari bahagian sokongan teknologi pemerintah atau perniagaan.
- Mereka akan:
  - Meminta maklumat peribadi anda, atau
  - Meminta anda memuat turun perisian yang akan memberikan mereka kawalan ke atas peranti dan maklumat anda, atau
  - Meminta anda agar tidak menyemak SMS, e-mel atau akaun bank anda selama 24 jam seterusnya

Contoh penipuan panggilan telefon dengan Tanda Awalan "+":



> Helo, saya dari bahagian **sokongan teknologi** syarikat XX. Komputer anda memaklumkan kepada kami bahawa ia telah **dijangkiti virus dan perisian pengintip**. Sila **muat turun perisian ini sekarang** untuk mengelakkan komputer anda dikunci dalam masa **5 minit seterusnya**.

Penipuan E-Dagang

- Penipu menarik minat anda dengan harga yang rendah;
- Meminta anda membuat bayaran terlebih dahulu atau memberitahu anda bayaran telah dibuat.

Contoh mesej penipuan:

> Saya telah membayar barang anda tetapi wang tersebut **dikunci pada akaun anda**. Anda perlu **menyemak e-mel** yang telah saya hantar ke akaun e-mel anda untuk **menerima wang tersebut**.

Memancing data ialah kaedah yang digunakan oleh penjenayah siber untuk memperdayakan mangsa dengan memberikan maklumat peribadi dan kewangan anda seperti kata laluan, Kata Laluan Sekali (OTP) atau nombor akaun bank.

Ketahui 6 tanda memancing data

1. 

Penggunaan Bahasa Berunsurkan Desakan atau Ancaman

2. 

Menjanjikan Ganjaran Menarik

3. 

Meminta Maklumat Sulit

4. 

Maklumat Tidak Sepadan & Mengelirukan

5. 
E-mel yang Tidak Dijangka

6. 
Lampiran yang Meragukan

https://go.gov.sg/csa-spotssignsofphishing

Perkara yang Boleh dilakukan & Tidak Boleh dilakukan untuk melindungi diri daripada penipuan dalam talian

1. Membenarkan pengesahan 2-faktor (2FA) sekiranya tersedia. Selain perbankan internet, 2FA juga tersedia untuk media sosial, e-mel, membeli-belah dan akaun pemerintah.
2. Sentiasa mengesahkan panggilan atau mesej yang mencurigakan dengan menelefon talian penting rasmi pemerintah/perniagaan atau aplikasi/laman web rasmi secara langsung.
3. Sekiranya mesej daripada keluarga dan rakan anda mencurigakan, hubungi mereka secara langsung untuk menyemak sama ada mereka telah menghantar mesej tersebut.
4. Tetapkan kata laluan yang kukuh dengan menggunakan huruf besar dan huruf kecil, nombor dan simbol. Gunakan perkataan yang berkaitan dengan memori yang unik bagi anda untuk membentuk sebuah Frasa, contohnya, **IhadKAYAtoastAT8AM**!
5. Muat turun dan pasang aplikasi scamshield dari Apple APP Store. *(Untuk Android, akan ada tidak lama lagi).* https://go.gov.sg/scamshield-setupguide

Senarai laman web berkaitan dengan pemerintah yang dipercayai boleh didapati di **www.gov.sg/trusted-sites**.

Lawati laman web **www.scamalert.sg** untuk mendapatkan maklumat lanjut atau hubungi talian bantuan Anti-Scam di **1800-722-6688** untuk mendapatkan nasihat berkaitan penipuan.

1. **JANGAN** segera mengklik pautan dalam mesej atau e-mel yang mendakwa daripada pemerintah atau daripada perniagaan yang sah apabila anda menerimanya.
2. **JANGAN** kongsi maklumat peribadi atau kewangan, kata laluan dan OTP anda.
3. **JANGAN** terus hubungi pengirim melalui butiran hubungan yang diberikan dalam e-mel atau mesej teks. Periksa nombor telefon di laman web rasmi terlebih dahulu.
4. **JANGAN** panik apabila anda menerima iklan atau mesej segera tanpa diminta untuk mengikuti beberapa arahan. Padam dan sekat pengguna, serta laporkan mesej pada platform tersebut.

Credit: Singapore Police Force and Cyber Security Agency of Singapore

An initiative by:

INFOCOMM MEDIA DEVELOPMENT AUTHORITY

Supported by:

SG :DIGITAL OFFICE