Lebih Selamat Siber Daripada Menyesal

Jenis-jenis penipuan secara dalam talian

1 Penipuan penyamaran

Berpura-pura sebagai pekerja dari pertubuhan dikenali seperti agensi-agensi pemerintah, bank atau syarikat telekomunikasi, penjenayah ini akan cuba mencuri wang anda melalui panggilan telefon, WhatsApp atau SMS.

Mereka akan meminta anda untuk:

- ikuti arahan segera yang mendakwa bahawa peranti anda telah digodam atau mempunyai masalah teknikal
- berikan butir-butir peribadi, perincian perbankan dan OTP (Kata Laluan Guna Sekali) kerana masalah dengan akaun bank anda, atau untuk mendaftar bagi tawaran palsu atau cabutan bertuah

Daripada: Bank XYZ

Kami telah mengesan aktiviti yang mencurigakan di akaun anda. Sila sahkan peranti ini dengan segera, ikuti pautan berikut: XYZ-bank.-com/sg/online-banking/?6512345678

Mereka juga boleh berpura-pura menjadi rakan, rakan sekerja atau ahli keluarga dan menghubungi anda di akaun media sosial atau WhatsApp. Mereka akan mendakwa bahawa anda telah memenangi hadiah, atau mendaftar anda untuk cabutan bertuah, dan meminta anda untuk:

- beri maklumat peribadi; atau
- Mengirim mereka OTP secara tidak sengaja

2 Penipuan e-dagang

Penjenayah siber juga memikat anda dengan tawaran murah. Mereka akan mendesak pembayaran segera, pemindahan bank sebelum penghantaran atau meminta untuk melakukan transaksi di luar platform. Selepas menerima wang anda, mereka tidak dapat dihubungi.

Jangan jadi mangsa jenayah siber. Ini caranya.

- **JANGAN** kongsi maklumat peribadi atau kewangan, kata laluan dan OTP
- **JANGAN** hubungi pengirim secara langsung melalui maklumat hubungan yang diberikan dalam e-mel atau mesej. Lakukan melalui maklumat hubungan yang tertera di laman web rasmi
- **JANGAN** mempercayai pautan atau alamat e-mel yang mendakwa berasal dari pemerintah tetapi tidak mempunyai "**gov.sg**" di dalamnya, kecuali jika anda sudah biasa dengannya. Senarai laman web berkaitan pemerintah yang dipercayai boleh didapati di **www.gov.sg/trusted-sites**
- **JANGAN** panik apabila anda menerima iklan atau mesej mendesak yang tidak diminta untuk mengikuti beberapa arahan. Hubungi ahli keluarga atau rakan anda untuk mendapatkan nasihat. Layari **www.scamalert.sg** untuk maklumat lebih lanjut atau hubungi talian bantuan Anti-Scam di **1800-722-6688** untuk dapatkan nasihat berkaitan penipuan

Apakah pancingan data?

Penjenayah siber biasanya menggunakan kaedah yang disebut "pancingan data" untuk menipu mangsa agar memberi maklumat peribadi seperti nombor akaun bank, perincian log masuk seperti kata laluan dan OTP.

Ketahui 6 tanda-tanda pancingan data

1

Maklumat Tidak Tepat & Mengelirukan

2

E-mel yang tidak dijangka

3

Bahasa yang mendesak atau mengancam

4

Lampiran Mencurigakan

5

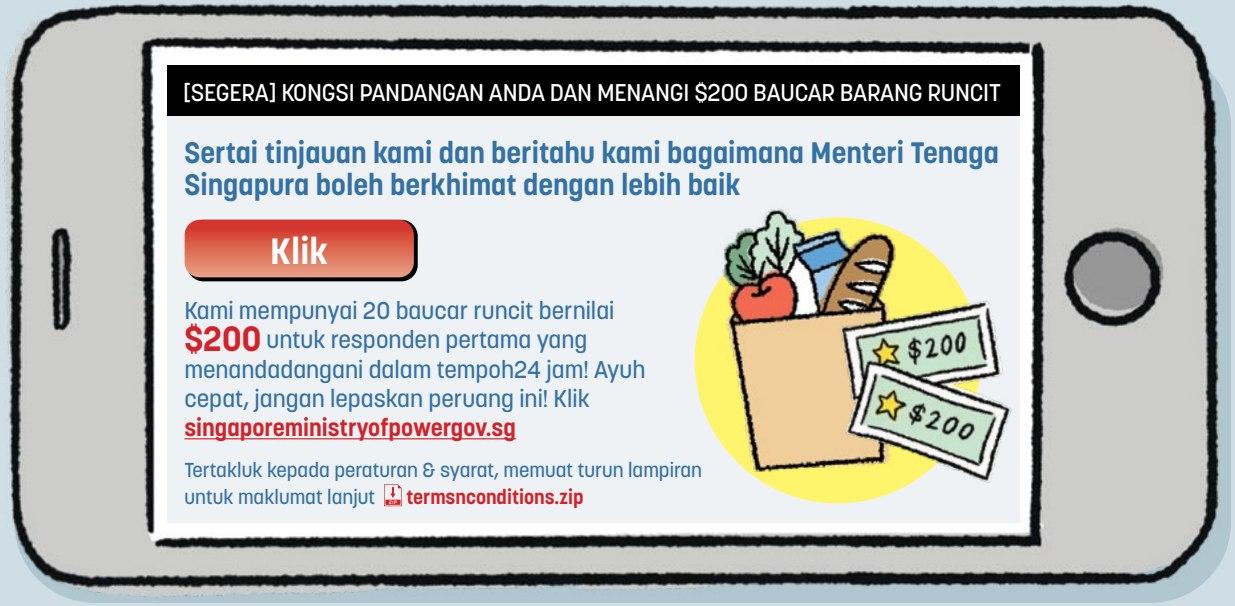
Janji Hadiah Menarik

6

Permintaan bagi Maklumat Rahsia

Kegiatan:

Cara kesan kegiatan pancingan data



Adakah anda lihat 6 tanda-tanda itu?

- Penggunaan bahasa mendesak
- Janji bagi tawaran yang menarik
- kesalahan ejaan
- Kementerian yang tidak wujud di Singapura
- Maklumat Tidak Tepat & Mengelirukan
- Lampiran mencurigakan

Better cyber safe than sorry

Bagi maklumat lanjut, sila lawati lelaman Agensi Keselamatan Siber Singapura (CSA) dan Scam Alert.

www.csa.gov.sg **www.scamalert.sg**

Dapatkan lebih banyak nasihat siber di:

Bagi maklumat penipuan terbaru, lawati: