பின்னர் வருந்தாமல் இப்போதே இணையத்தில் பாதுகாப்பாக இருங்கள்

CSA SINGAPORE

SINGAPORE POLICE FORCE
SAFEGUARDING EVERY DAY

இணைய மோசடி வகைகள்

1 ஆள்மாறாட்ட மோசடிகள்

இந்தக் குற்றவாளிகள் உங்களைத் தொலைபேசியில் அழைத்து, வாட்ஸ்ஆப் அல்லது குறுந்தகவல் அனுப்பி, அரசாங்க அமைப்புகள், வங்கிகள் அல்லது தொலைத்தொடர்பு நிறுவனங்கள் போன்ற நன்மதிப்புள்ள அமைப்புகளின் ஊழியர்களைப் போல பாசாங்கு செய்து, உங்கள் பணத்தைத் திருட முயற்சி செய்வார்கள்.

இவர்கள் உங்களிடம் பின்வருமாறு சொல்வார்கள்:

- உங்களது சாதனங்களில் ஊடுருவல் ஏற்பட்டிருப்பதால் அல்லது தொழில்நுட்பப் பிரச்சனைகள் இருப்பதால் உடனடியாக அறிவுறுத்தல்களைப் பின்பற்றவேண்டும்

- உங்கள் வங்கிக் கணக்கில் பிரச்சனை ஏற்பட்டிருப்பதால், அல்லது போலிச் சலுகைகள், அதிர்ஷ்டக் குலுக்கல்கள் போன்றவற்றுக்குப் பதிவு செய்வதற்காக, உங்களது தனிப்பட்ட விவரங்கள், இணைய வங்கிச்சேவை விவரங்கள், ஒருமுறை பயன்படுத்தும் கடவுச்சொற்கள் ஆகியவற்றை நீங்கள் தெரிவிக்கவேண்டும்

> அனுப்புநர்: XYZ வங்கி
>
> உங்கள் கணக்கில் சந்தேகத்திற்குரிய நடவடிக்கையைக் கண்டு பிடித்திருக்கிறோம். தயவுசெய்து இந்த இணைப்பைப் பயன்படுத்தி சாதனத்தை உடனடியாக உறுதி செய்யுங்கள்:
> XYZ-bank.-com/sg/online-banking/?6512345678

அவர்கள் உங்களது நண்பர்களாக, சக ஊழியர்களாக அல்லது குடும்ப உறுப்பினர்களாகவும் பாசாங்கு செய்து, சமூக ஊடகக் கணக்குகளில் அல்லது வாட்ஸ்ஆப்பில் உங்களுடன் தொடர்பு கொள்ளக்கூடும். உங்களுக்குப் பரிசு கிடைத்திருப்பதாக, அல்லது அதிர்ஷ்டக் குலுக்கலுக்கு உங்களைப் பதிவு செய்வதாகச் சொல்லி, பின்வருமாறு சொல்வார்கள்:

- உங்களது தனிப்பட்ட விவரங்களை நீங்கள் தெரிவிக்கவேண்டும்; அல்லது

- தவறுதலாக உங்களுக்கு அனுப்பப்பட்ட ஒருமுறை பயன்படுத்தும் கடவுச்சொல்லை அவர்களுக்கு அனுப்பி வைக்கவேண்டும்

2 இணைய விற்பனை மோசடிகள்

இணையக் குற்றச்செயல்களைப் புரிவோர் மலிவான சலுகைகளுடன் உங்களுக்கு ஆசை காட்டுவார்கள். உடனடியாகப் பணம் செலுத்தும்படியும், பொருளை அனுப்பி வைப்பதற்குமுன் வங்கி பணமாற்றம் செய்யும்படியும் வற்புறுத்துவார்கள் அல்லது இணையத்திற்கு அப்பால் பரிவர்த்தனை செய்ய கோரிக்கை விடுப்பார்கள். உங்கள் பணத்தைப் பெற்றுக்கொண்ட பிறகு அவர்களுடன் தொடர்புகொள்ள இயலாமல் போய்விடும்.

இணையக் குற்றச்செயலுக்கு இலக்காகாதீர்கள். அதற்கான வழிகாட்டிகள்.

- உங்களது தனிப்பட்ட அல்லது நிதித் தகவல்கள், கடவுச்சொற்கள், ஒருமுறை பயன்படுத்தும் கடவுச்சொற்கள் எதனையும் யாரிடமும் சொல்லாதீர்கள்

- மின்னஞ்சலில் அல்லது குறுந்தகவலில் கொடுக்கப்பட்டுள்ள தொடர்பு விவரங்களின் வாயிலாக அனுப்பியவரை நேரடியாக அழைக்காதீர்கள். அதிகாரபூர்வ இணையத்தளத்தில் உள்ள தொடர்பு விவரங்களின் வாயிலாக மட்டுமே தொடர்பு கொள்ளுங்கள்

- அரசாங்கத்தால் அனுப்பப்பட்டதாகச் சொல்லிக்கொள்ளும் இணைப்புகளில் அல்லது மின்னஞ்சல் முகவரிகளில் “gov.sg” இல்லாவிட்டால், அவை உங்களுக்குப் பழக்கப்பட்டவையாக இருந்தாலொழிய அவற்றை நம்பாதீர்கள். நம்பகமான அரசாங்கம் சார்ந்த இணையத்தளங்களின் பட்டியலை **www.gov.sg/trusted-sites** இணையத்தளத்தில் காணலாம்

- கேட்கப்படாத அவசர விளம்பரம் அல்லது சில அறிவுறுத்தல்களைச் செய்யச் சொல்லும் தகவல் உங்களுக்குக் கிடைத்தால் பதறாதீர்கள். உங்கள் குடும்பத்தினரை அல்லது நண்பர்களை அழைத்து ஆலோசனை கேளுங்கள். மேல்விவரம் அறிய **www.scamalert.sg** இணையத்தளத்தை நாடுங்கள் அல்லது மோசடி தொடர்பான ஆலோசனைக்கு **1800-722-6688** என்ற மோசடித்தடுப்பு தொலைபேசி சேவையை அழையுங்கள்

தகவல் திருட்டு என்பது என்ன?

இணையக் குற்றச்செயல்களைப் புரிவோர், “தகவல் திருட்டு” (phishing) எனும் தந்திரத்தைப் பயன்படுத்தி, வங்கிக் கணக்கு எண்கள், கடவுச்சொற்களும் ஒருமுறை பயன்படுத்தும் கடவுச்சொற்களும் உள்ளடங்கும் புகுபதிவு விவரங்கள் போன்ற தனிப்பட்ட, நிதித் தகவல்களை வெளியிட வைப்பார்கள்.

தகவல் திருட்டின் 6 அறிகுறிகளைத் தெரிந்து கொள்ளுங்கள்

1

பொருந்தாத மற்றும் தவறாக வழிநடத்தக்கூடிய தகவல்கள்

2

எதிர்பாராத மின்னஞ்சல்கள்

3

அவசரமான அல்லது அச்சுறுத்தும் வகையிலான சொற்களைப் பயன்படுத்துதல்

4

சந்தேகத்திற்குரிய இணைப்புகள்

5

கவர்ச்சிகரமான வெகுமதிகளைத் தருவதாக உத்தரவாதம் அளித்தல்

6

இரகசியத்தன்மை வாய்ந்த தகவல்களைக் கோருதல்

நடவடிக்கை:

தகவல் திருட்டின் அறிகுறிகளைக் கண்டுகொள்ளுங்கள்

6 அறிகுறிகளை அடையாளம் கண்டீர்களா?

- அவசரமான சொற்களின் பயன்பாடு
- கவர்ச்சிகரமான வெகுமதிகளைத் தருவதாக உத்தரவாதம்
- இலக்கணப் பிழைகள்
- சிங்கப்பூரில் இல்லாத அமைச்சு
- பொருந்தாத தகவல்கள்
- சந்தேகத்திற்குரிய இணைப்புகள்

Better cyber safe than sorry

மேல்விவரம் அறிய, சிங்கப்பூர் இணையப் பாதுகாப்பு அமைப்பு மற்றும் மோசடி எச்சரிக்கை இணையத்தளத்தை நாடுங்கள்.

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

இன்னும் பல இணையக்குறிப்புகளுக்கு:

மோசடி பற்றிய அண்மைத் தகவலுக்கு, பாருங்கள்: