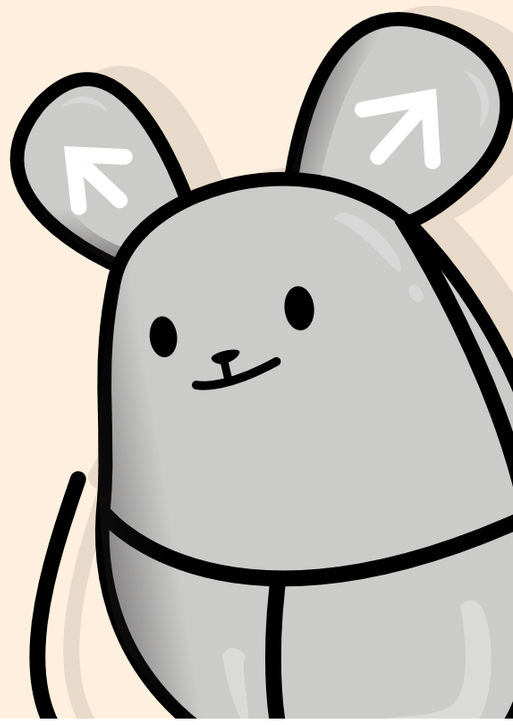
பாதுகாப்பாக இருங்கள்

உங்களின் தனிப்பட்ட தரவுகளைப் பாதுகாத்துக் கொள்ளுங்கள்



தனிப்பட்ட தரவுகள் என்பவை ஒரு தனிநபர் யார் என்பதை அடையாளம் காண்பிக்கக்கூடிய தகவல்களாகும். அவற்றில் உள்ளடங்கக்கூடிய உங்கள் தகவல்கள்:

- பெயர்
- பிறந்த தேதி
- அடையாள அட்டை எண்
- கடவுச்சீட்டு எண்
- முகவரி
- தொலைபேசி எண்
- இருப்பிடத் தரவுகள்
- வங்கிக் கணக்கு மற்றும் கடன் அட்டை எண்கள்
- கணக்கின் பயனர் பெயர்கள் மற்றும் கடவுச்சொற்கள்

இவை எவ்வாறு தவறாகப் பயன்படுத்தப்படலாம்?

இணையக் குற்றவாளிகள் இந்தத் தரவுகளைப் பல வழிகளில் திருடிப் பயன்படுத்தலாம். அவற்றில் உள்ளடங்குவன:

உங்கள் கணக்குகளை அணுகுதல்

மோசடி செய்து பொருட்களை வாங்குதல்

உங்களைப் போல் நடித்து ஆள்மாறாட்டம் செய்தல், உங்களைப் பின்தொடர்தல் அல்லது மிரட்டிப் பணம் பறித்தல்

நான் எதற்காக இதைத் தெரிந்துகொள்ள வேண்டும்?

- தொழில்நுட்பம் சார்ந்த மோசடிகள் மூலம் 2020 ஜனவரி முதல் ஏப்ரல் வரை $7.7 மில்லியன் டாலர் ஏமாற்றப்பட்டுள்ளது. இவற்றில், இணையக் குற்றவாளிகள் பாதிக்கப்பட்டவர்களிடம் இணைய இணைப்புப் பிரச்சினைகளைத் தீர்ப்பதாக அல்லது இணைய ஊடுருவல் (ஹேக்கிங்) சம்பவத்தை விசாரிப்பதாகப் போலியான காரணத்தைக் கூறி அவர்களின் கணினிகளில் "மென்பொருள் பயன்பாடுகளை" நிறுவியுள்ளனர்.
- அதன் பிறகு, மோசடி செய்பவர்கள் நிறுவப்பட்ட தீங்கிழைக்கும் மென்பொருள் மூலம் பாதிக்கப்பட்டவர்களின் தனிப்பட்ட தரவுகளைப் பெற்று, அவற்றைத் தவறான வழிகளில் பயன்படுத்தியுள்ளனர்.
- நடைபெற்ற பிற சம்பவங்களில், பாதிக்கப்பட்டவர்கள் மின்னிலக்க நச்சுப்பெருக்கிகள் (Digital Worms) அல்லது 'டிரோஜான்' எனப்படும் தீங்கிழைக்கும் மென்பொருளைக் கொண்ட இணைப்புகளைக் 'கிளிக்' செய்ததன் மூலம் ஏமாற்றப்பட்டனர். அவற்றால் ஒரு நபரின் தரவுகளை நகலெடுக்கவோ, நீக்கவோ அல்லது மாற்றவோ முடியும்.

1CLICK AWAY
Be Safe · Be Smart · Be Kind

MEDIA LITERACY COUNCIL

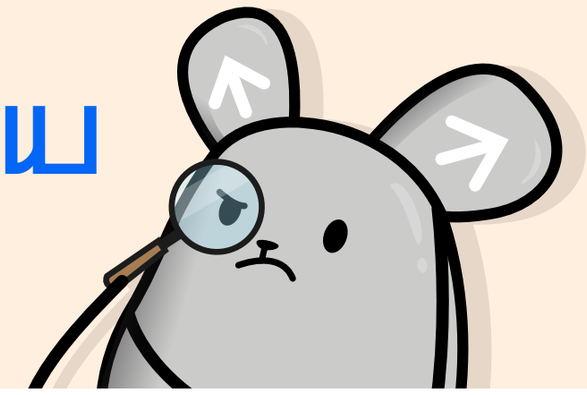
#பாதுகாப்பாக இருங்கள்

கிளிக் செய்வதற்கு முன்னர் சரிபார்க்கவும்

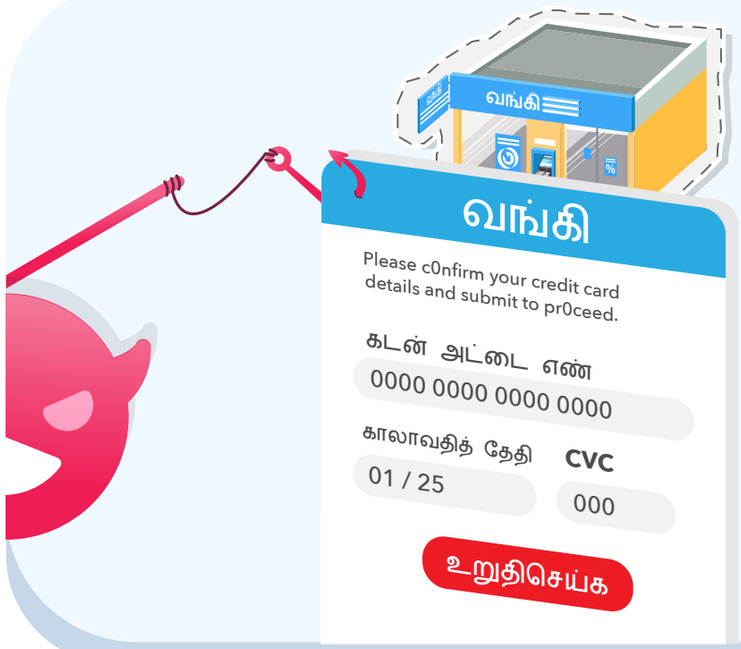
ஆதரவளித்தவர்:
INFOCOMM MEDIA DEVELOPMENT AUTHORITY
CSA SINGAPORE
SINDA Singapore Indian Development Association

இவரது ஆதரவுடன்:
SG:D | GET READY!

எனது தரவுகள் திருடப்படக்கூடிய சில வழிகள் யாவை?



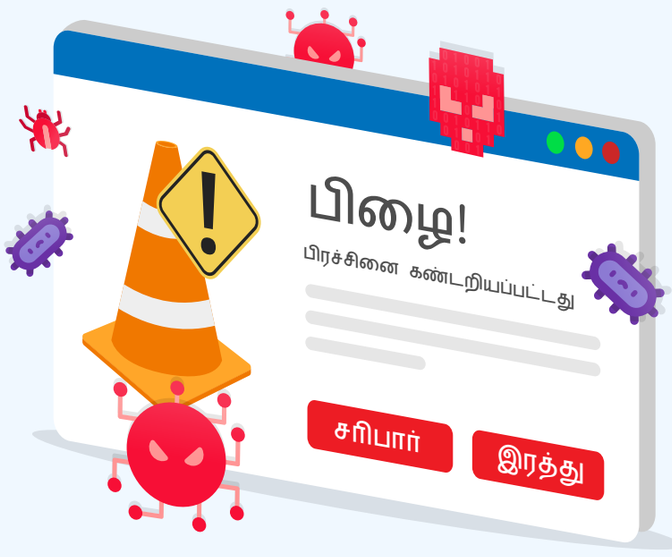
நீங்கள் கவனமாக இருக்க வேண்டிய சில விஷயங்கள் இங்கே கொடுக்கப்பட்டுள்ளன!



பிஷிங் (மோசடி மின்னஞ்சல்)

மோசடி செய்பவர்கள் உங்களின் உள்நுழைவு விவரங்கள், வங்கிக் கணக்கு, கடன் அட்டை எண்கள் போன்ற தனிப்பட்ட அல்லது நிதி சார்ந்த தகவல்களை உங்களிடம் இருந்து ஏமாற்றிப் பெறுவதற்கு பிஷிங் (Phishing) பயன்படுத்தப்படுகிறது.

இது போலி மின்னஞ்சல்கள், தொலைபேசி செய்திகள் அல்லது உண்மையான நிறுவனங்களைப் போன்று தோற்றம் தரும் வலைத்தளங்களின் வடிவத்தில் இருக்கலாம்



மால்வேர்

மால்வேர் என்பது தீங்கிழைக்கும் மென்பொருளாகும். இது உங்கள் சாதனங்களை முடக்கலாம் அல்லது உங்கள் தரவுகளைத் திருடலாம்.

மால்வேரைக் கொண்டிருக்கும் மின்னஞ்சல்கள் அல்லது செய்திகளில் உள்ளடங்கியிருக்கும் சந்தேகத்திற்குரிய இணைப்புகள் அல்லது பின்னிணைப்புகளைக் கிளிக் செய்ய வைப்பதற்கு மோசடி செய்பவர்கள் உங்களைக் கவர்ந்திழுக்கலாம்.

ஊடுருவல் (ஹேக்கிங்)

மோசடி செய்பவர் பாதுகாப்பற்ற வை-ை வலையமைப்புகளை இடைமறிக்கலாம். இது உங்கள் கோப்புகளை அணுக அல்லது உங்கள் இணையவழிச் செயல்பாட்டைப் பின்தொடர அனுமதிக்கிறது.

#பாதுகாப்பாக இருங்கள்

கிளிக் செய்வதற்கு முன்னர் சரிபார்க்கவும்

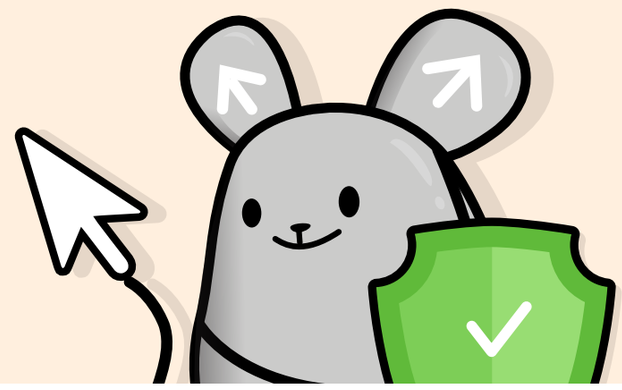
1CLICK AWAY
Be Safe · Be Smart · Be Kind

MEDIA LITERACY COUNCIL

ஆதரவளித்தவர்:
INFOCOMM MEDIA DEVELOPMENT AUTHORITY
CSA SINGAPORE
SINDA Singapore Indian Development Association

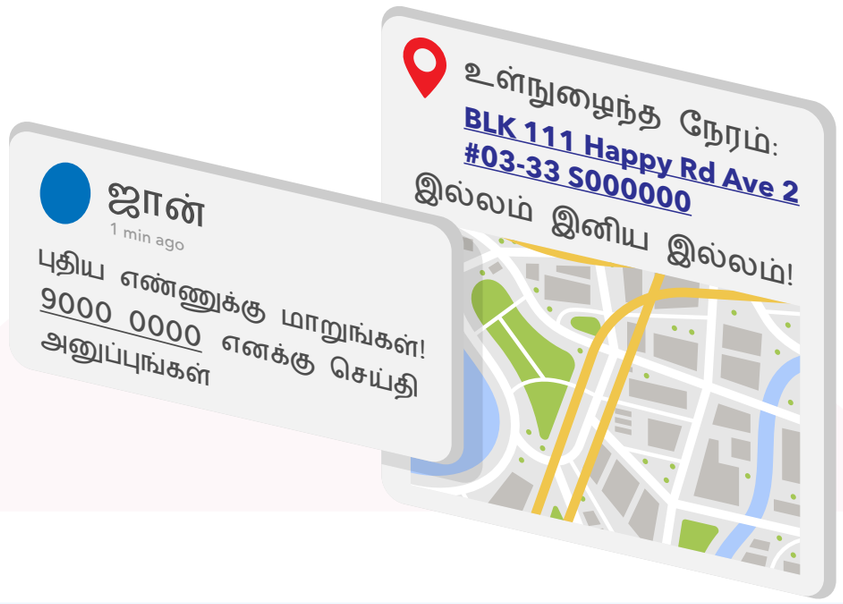
இவரது ஆதரவுடன்:
SG:D | GET READY!

எனது தனிப்பட்ட தரவுகளை நான் எவ்வாறு பாதுகாக்கலாம்?



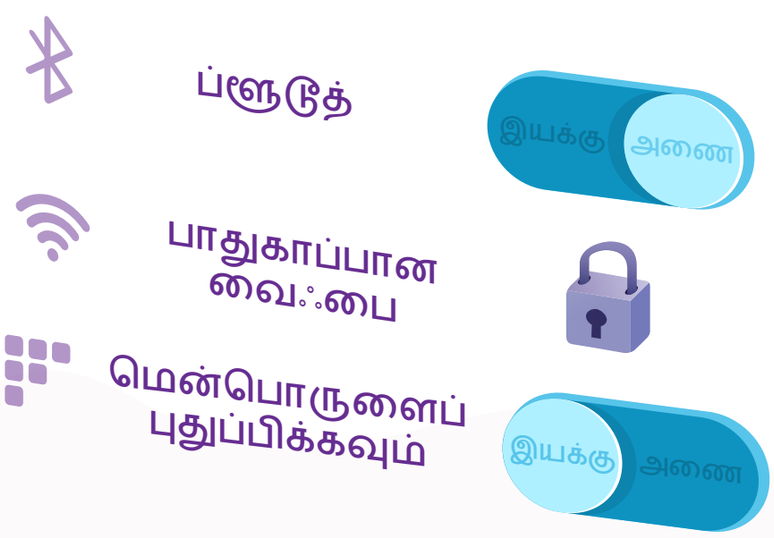
உங்கள் தனிப்பட்ட தரவுகளை இணையத்தில் பாதுகாக்க இங்கே சில பாதுகாப்பான மின்னிலக்கப் பழக்கவழக்கங்கள் குறித்து தெரிவிக்கப்பட்டுள்ளன !

- உங்கள் வீட்டு முகவரி அல்லது தொலைபேசி எண் போன்ற தொடர்புத் தகவல்களைப் பதிவிடுவதைத் தவிர்க்கவும்.
- உங்கள் வங்கி மற்றும் தனிப்பட்ட விவரங்களை உங்கள் சாதனத்தில் சேமிக்க வேண்டாம். ஒவ்வொரு பரிவர்த்தனைக்குப் பிறகும் வெளியேறுவதை நினைவில் கொள்ளவும்.



- உங்களின் தனிப்பட்ட தரவுகளைக் கோருகின்ற, இணைப்பைக் கிளிக் செய்யும்படி உங்களைக் கேட்கின்ற அல்லது இணைப்பைப் பதிவிறக்கும்படி உங்களைத் தூண்டுகின்ற வேண்டப்படாத மின்னஞ்சல்கள் அல்லது செய்திகளிடம் எச்சரிக்கையாக இருங்கள்.
- மோசடி செய்பவர்கள் உங்கள் நம்பிக்கையைப் பெறுவதற்காகப் பெரும்பாலும் அரசாங்க அதிகாரிகள் அல்லது பிரபலமான வணிகங்களின் (எ.கா. வங்கிகள் மற்றும் தொலைத்தொடர்பு நிறுவனங்கள்) பிரதிநிதிகளைப் போல ஆள்மாறாட்டம் செய்கிறார்கள். அனுப்புநரின் நம்பகத்தன்மையை உங்களால் உறுதிப்படுத்திக்கொள்ள முடியாவிட்டால், எந்த இணைப்புகளிலும் பதிலளிக்கவோ அல்லது கிளிக் செய்யவோ வேண்டாம்.

- பயன்பாட்டில் இல்லாதபோது உங்கள் சாதனங்களில் உள்ள புளூடூத்தை அணைக்கவும். ஏனெனில் இது கணினி ஊடுருவிகளுக்கு (Hacker) பாதுகாப்பு பலவீனங்களைக் கண்டறிவதற்கான வழியை உருவாக்கலாம்.
- வலுவான கடவுச்சொற்களைப் பயன்படுத்தவும். மேலும், கிடைக்குமிடத்தில், கூடுதல் பாதுகாப்புக்கு இரு-காரணி அங்கீகாரத்தைச் (2FA) செயற்படுத்தவும்.
- பாதுகாப்பற்ற வை-ஃபை வலையமைப்புகளில் தனிப்பட்ட அல்லது இரகசியத் தகவல்கள் உள்ளடங்கிய பரிவர்த்தனைகளை மேற்கொள்ள வேண்டாம்.
- புதிய பதிப்புகள் கிடைத்தவுடன் உங்கள் சாதனங்களில் உள்ள மென்பொருள் மற்றும் செயலிகள் அனைத்தையும் புதுப்பிக்கவும். இது பிழைகளைச் சரிசெய்கிறது, மேலும் புதிய நச்சுநிரல்கள் மற்றும் மால்வேர்களை எதிர்த்துப் போராடுவதற்குப் பாதுகாப்புக் குறைபாடுகளை நீக்குகிறது.



#பாதுகாப்பாக இருங்கள்

கிளிக் செய்வதற்கு முன்னர் சரிபார்க்கவும்

1CLICK AWAY
Be Safe · Be Smart · Be Kind

MEDIA LITERACY COUNCIL

ஆதரவளித்தவர்:
IMDA INFOCOMM MEDIA DEVELOPMENT AUTHORITY
CSA SINGAPORE
SINDA Singapore Indian Development Association

இவரது ஆதரவுடன்:
SG:D | GET READY!