பே.ஃஸ்புக்கை பாதுகாப்பாகக் கையாள்வது எப்படி?

பே.ஃஸ்புக் என்பது உலகப் பிரசித்தி பெற்ற ஒரு சமூக வலைத்தளமாகும். சமூக வலைத்தளம் என்பது இணையம் மூலமாக ஒருவர் மற்றவர்களுடன் சமூகத் தொடர்புகளைப் பேணும் ஒரு முறையாகும்.
இதன் மூலம் நிழற்படங்கள் பரிமாற்றம், நிகழ்ப்படங்கள் பரிமாற்றம், அன்றாடம் நடைபெற்ற நிகழ்வுகள் பற்றிய விடயங்கள் பரிமாற்றம் பொன்றவை அதிகமாக நடைபெறும் செயல்களாகும். தற்போது 300 மில்லியனுக்கும் அதிகமான நபர்கள் பே.ஃஸ்புக்கைப் பயன்படுத்துவதாகவும் சராசரியாக ஒரு நாளில் 6 பில்லியன் நிமிடங்களுக்கும் மேல் பே.ஃஸ்புக்கில் காலம் கழிப்பதாகவும் புள்ளிவிவரங்கள் தெரிவிக்கின்றன.

சமீபத்தில் மேற்கொள்ளப்பட்ட கருத்தாய்வுகளின்படி, கீழ்க்காணும் விடயங்கள் பே.ஃஸ்புக்கின் நன்மதிப்புக்கிற்கான காரணிகளாக அடையாளம் காணப்பட்டுள்ளன.

- தடையின்றி நிழற்படங்கள் மற்றும் நிகழ்ப்படங்களைப் பே.ஃஸ்புக் வலைத்தளத்தினுல் மேலேற்றுவதற்கும், நண்பர்களுக்கிடையேயும் பரிமாற்றம் செய்வதற்கும் இயலுமை
- உறுப்பினர்கள் அன்றாடம் ஒவ்வொரு நிமிடமும் தமது நண்பர்கள் ஈடுபட்டிருக்கும் செயற்பாடுகள் பற்றி அறிந்துகொள்ள இயலுமை
- பே.ஃஸ்புக்கினுள் இருக்கும் தமது நண்பர்களுடன் இணையம் சார்ந்த விளையாட்டுக்களில் ஈடுபடுதல்
- தமது நண்பர்க்கு இ-பரிசு (மின்-பரிசு) களை அனுப்பும் வசதி

இத்தனை அனுகூலங்கள் இருக்கின்ற போதும் எந்தவொரு தொழில்நுட்பத்திலும் குறைபாடுகள் இருப்பது போன்று பே.ஃஸ்புக்கிலும் தனிநபரின் சுதந்திரம் பற்றியப் பிரச்சினைகள் உள்ளன. கடந்த 3-4 வருடங்களில் பே.ஃஸ்புக் பாவனையாளர்களைக் குறிக்கோளாகக் கொண்டு நடத்தப்படும் அத்துமீறல்கள் அதிகரித்திருப்பதோடு தனிநபர் அந்தரங்கத்திற்கு அச்சுறுத்தலாகவும் அமைந்துள்ளது.

இணையம் சார்ந்துள்ள சமூக வலையமைப்பு உங்களைப் பற்றியும், உங்கள் செயற்பாடுகள் குறித்தும், நீங்கள் இருக்குமிடம் மற்றும் நீங்கள் தொடர்பு கொள்ளும் நபர்கள் பற்றிய விபரங்களை ஏனையோர் அறிந்து கொள்ள வழிவகுக்கிறது. இத்தகவல்கள் சிலவேளை உங்கள் உயிருக்கே ஆபத்து விளைக்கலாம்.

பே.ஃஸ்புக் போன்ற சமூக வலையமைப்பைச் சார்ந்த இணையத் தளங்களில் பாதுகாப்பாகப் பவனி வருவதற்கு நாம் பல வழிகளைக் கையாளலாம். அத்தகைய அணுகு முறைகளைக் கீழே காண்க:

1. https://www.facebook.com என்ற URL க் கொண்டு பே.ஃஸ்புக்கினுள் பிரவேசியங்கள். இதன் மூலம் உங்கள் ரகசிய வார்த்தையைத் (password) திருடி உங்கள் இணைய பக்கத்தினுள் நுழைய முற்படும் நபர்களிடமிருந்து பாதுகாத்துக் கொள்ளலாம்.
2. குறுந்தகவல் (SMS) சார்ந்த உறுதிப் படுத்தும் முறையைக் கையாள்தல். (இந்த முறையைக் கையாளும் போது பே.ஃஸ்புக்கினுள் பிரவேசிப்பதற்கு முன் குறுந்தகவல் மூலம் உட்செலுத்தவேண்டிய ஒரு குறியீடு அனுப்பப்படும்).
3. உங்களின் தனிப்பட்ட விடயங்கள் பற்றிய தகவல்களைப் பே.ஃஸ்புக்கிற்கு வழங்குவதை முடிந்தவரைத் தவிர்த்துக் கொள்ளுங்கள். (முக்கியமாக உங்கள் முகவரி, பிறந்த திகதி போன்றவை). ***தனியுரிமை அமைப்பு*** *(Privacy setting)* மூலம் பகிரங்கப் படுத்தப்படும் தகவல்களை மட்டுப்படுத்தலாம்.
4. ஒவ்வொரு தடவையும் பே.ஃஸ்புக்கினுள் பிரவேசிக்கும் போது உங்களது மின்னஞ்சலுக்கு ஒரு தகவல் (notification) அனுப்பும் வகையில் தனியுரிமை அமைப்பில் மாற்றங்கள் செய்யவாம்.
5. புது நண்பர்களை இணைத்துக் கொள்ளும் போது முதலில் மட்டுப்படுத்த விதத்தில் உங்கள் விபரங்கள் அவர்களுக்குத் தென்படும் விதத்தில் தனியுரிமை அமைப்பினை மாற்றம் செய்யுங்கள். புதியவர்களை இணைத்துக் கொண்டதன் பின் அவர்களின் நடவடிக்கைகள் பற்றி விழிப்புடன் இருங்கள்.
6. பே.ஃஸ்புக் போன்ற தோற்றம் கொண்ட போலி இணைய தளங்கள் உள்ளதால் தகவல்களை வழங்குவதற்கு முன் எச்சரிக்கையுடன் கையாளுங்கள்.

பிஷிங் மின்னஞ்சல் என்பது பயனாளர் க்ளிக் செய்தவுடன் அவர் அறியாமலே வைரஸ் தானாகவே இறக்கம் செய்யப்பட்டு கனணியினுள் ஸ்தாபிதம் செய்துகொள்வதற்காகவே உருவாக்கப்பட்டதாகும்.

உங்களது (வலைத்தளத்தினுள்) உட்செல்லும் தகவல்களைத் திருடும் நோக்கில் தயாரிக்கப்பட்ட இணைப்புவரிகள் பே∴ஸ்புக் போன்ற தோற்றம் கொண்ட போலி இணையத்திற்கு உங்களை அழைத்துச் செல்லக் கூடும்.

நீங்கள் https://www.facebook.com URL லை பயன்படுத்தி பே∴ஸ்புக்கினுள் பிரவேசிக்கும் போது டிஜிடல் சான்றிதலைப் பரிசீலிப்பதின் மூலம் இணையத் தளத்தின் நம்பகத்தன்மையை உறுதி செய்து கொள்ள முடியும். பே∴ஸ்புக் வோல் (facebook wall), பீ∴ட்ஸ் (feeds), மற்றும் செய்திகளில் (Messages) காணப்படும் இணைப்புவரியின் மீது க்ளிக் செய்யும் போதும் இதைப் போன்ற நிகழ்வு நடைபெறக் கூடும்.

7. ஒரு நபரை நண்பனாகவோ நண்பியாகவோ இணைத்துக் கொள்வதற்கு முன் நன்கு யோசித்து முடிவெடுங்கள். அவர் உண்மையாகவே உங்களுக்குத் தோழமை அழைப்பு விடுத்துள்ளாரா என்பதை மின்னஞ்சல் மூலமோ அல்லது தொலைபேசி மூலமோ தொடர்பு கொண்டு உறுதி செய்து கொள்ளுங்கள்.
8. பே∴ஸ்புக் மூலம் சம்பாஷனை (Chatting) செய்யவும் இயலும். அறிமுகமில்லாத நபர்களுடன் சம்பாஷனை (chatting) செய்வதைத் தவிர்த்துக் கொள்ளுங்கள். மேலும் உங்களை அடையாளங்காட்டவல்ல தகவல்களைச் சம்பாஷனையின் போது ஒருபோதும் வழங்க வேண்டாம். யாராவது ஒருவர் தொல்லை தருபவராக இருந்தால் உடனே அவரை நண்பர் பட்டியலிலிருந்து விலக்கி விடுங்கள்.
9. எளிதில் ஊகிக்க முடியாத பலமானதொரு கடவுச்சொல்லை பயன்படுத்தவும். அத்தோடு அந்த கடவுச்சொல்லை அடிக்கடி மாற்றவும் மறந்து விடாதீர்கள். மேலும் உங்களது மின்னஞ்சலுக்கோ அல்லது வேறு எந்தவித இணைய அங்கத்துவத்திற்கோ ஒரே கடவுச்சொல்லைப் பயன்படுத்த வேண்டாம்.
10. எப்போதுமே நம்பகமான கணினியைப் பயன்படுத்துவதன் மூலம் மட்டுமே பே∴ஸ்புக்கினுள் பிரவேசம் செய்யுங்கள். ஏனெனில் அந்நிய கணினியைப் படுத்தும் போது அவற்றினுள் உங்கள் தட்டச்சு தரவுகளைக் கொள்ளையிடும் Key Loggers போன்ற கணினி நிரல்கள் இருக்கக்கூடும்.
11. உங்களது கடவுச்சொல்லை மற்றவரிடம் பகிர்ந்து கொள்ளும் போது கவனமாக இருங்கள். எளிதான கடவுச்சொல்லை உபயோகப் படுத்தினால் அதனை இலகுவாக கண்டு பிடித்துவிடக்கூடும்.

சமூக வலைத்தளம் மூலம் நீங்கள் பெறும் அனுபவம் உங்களை மகிழ்ச்சியின் உச்சத்திற்கு இட்டுச் செல்லக்கூடும். ஆனால் பலர் தன்னையும் தன் நண்பர்களையும் ஆபத்தில் இழுத்துவிடும் வகையில் பாதுகாப்பற்ற முறையில் செயற்படக்கூடும். ஆகவே TechCERT நிறுவனம் அறிவுறுத்தும் வகையில் செயற்படுவதன் மூலம் பே∴ஸ்புக் பாவனையின் போது ஏற்படும் பிரச்சினைகளை நாம் பெரும்பாலும் தவிர்த்துக் கொள்ளலாம்.
நீங்கள் பே∴ஸ்புக்கினைப் பயன்படுத்துபோது ஏற்படும் பிரச்சினைகள் சம்பந்தமாக ஆலோசனைகள் ஏதேனும் தேவைப்படின் கீழ்காணும் முகவரியில் காணப்படும் படிவத்தினை நிரப்பி எங்களுக்குத் தெரியப் படுத்துங்கள்.

If you have any questions, please inform us:

https://techcert.lk/en/report-form
தொலைபேசி - +94 11 4 462 562
மின்னஞ்சல் - help@techcert.lk

This document was prepared by the Training Division of LK Domain Registry in collaboration with the Internet Society Sri Lanka Chapter.
For more details please visit http://nic.lk/index.php/training-materials.

.LK Internet Society Sri Lanka Chapter TechCERT HELPING YOU SECURE YOUR INFORMATION ASSETS