ஒரு வலுவான கடவுச்சொல்லை உருவாக்குதல்

கடவுச்சொல் என்றால் என்ன?

- ஒரு இடத்திற்குள் நுழைய அனுமதி பெற பயன்படுத்தப்படும் இரகசிய சொல் கடவுச்சொல் ஆகும்.
- கடவுசொல்லானது ஒரு நபர் அல்லது பொருளுடன் தொடர்புடைய அவரின் அடையாளத்தை உறுதிப்படுத்தும் தகவல் ஆகும்.
- கடவுச்சொற்களை திருடுவதற்கு பல வழிகள் இருக்கின்ற போதிலும், வலுவான கடவுச்சொல்லை பயன்படுத்தி உங்களது தகவல்களை பாதுகாத்து கொள்ளலாம்.

கடவுச்சொற்கள் ஏன் தேவைப்படுகிறது?

-அனுமதியை அங்கீகரிப்பதற்காக (உறுதிசெய்தல்) கடவுச்சொற்கள் பயன்படுத்தப்படுகின்றன. கணினியில் உங்களை உங்கள் மின்னணு அடையாளத்துடன் இணைக்கும் நடவடிக்கையாக அங்கீகரித்தலை கருத முடியும்.

உங்கள் கடவுச்சொல்லானது பயனர் /கணக்கு அடையாளத்தை உறுதிப்படுத்தி முறையான உரிமையாளர் நீங்கள் என்பதை கணினியில் சரிபார்க்க பயன்படுத்தப்படுகிறது.
இது பொதுவாக புகுபதிகை(உள்நுழைவு) என குறிப்பிடப்படுகிறது.

நாம் அன்றாட வாழ்வில் பயன்படுத்தும் தனிநபர் அடையாள இலக்கங்கள்(PIN), கடவுச்சொற்கள், கடவுச்சொல் குறியீடுகளை நினைத்து பாருங்கள்.உங்கள் மின்னஞ்சலுக்குள் உள்நுழைய, உங்கள் கணினியை அணுக, தானியங்கி பணப்பரிமாற்ற இயந்திரத் திலிருந்து (ATM) பணம் எடுக்க, சமூக வலைத்தளங்களுக்குள் உள்நுழைய, மற்றும் பல காரணங்களுக்காக இவற்றை பயன்படுத்துகிறீர்கள். இவை அனைத்தையும் நினைவில் வைத்திருப்பது கடினமான செயலாகும்.

அத்துடன் எனது கணக்கை திருடவேண்டும் என்று யார் எண்ணுவார்கள் என்ற அலட்சியமான மன நிலையிலும் இருப்பீர்கள். ஆனால் உங்கள் கணக்கை திருடும் நபர் (Attacker) உங்கள் கணக்கிற்குள் உள் நுழைவதோடு மட்டுமல்லாது உங்கள் தரவுகளை பயன்படுத்தி பெரிய சேதத்தையும் விளைவிக்க கூடும். பொருத்தமான அல்லது தேவையான நபர்களுக்கு மாத்திரம் அணுக்கத்தினை(Access) கொடுப்பது உங்கள் தரவு மற்றும் தகவல்களை பாதுகாக்க உதவும். அதாவது இது உறுதிப்படுத்தல் என கூறப்படும். கடவுச்சொற்களை பயன்படுத்துவதே இதை செய்வதற்கு சிறந்த வழியாகும்.

ஒரு வலுவான கடவுச்சொல்லை எப்படி தேர்ந்தெடுப்பது?

அநேகமான நபர்கள் மிக இலகுவாக ஞாபகப்படுத்தும் சொற்களை கொண்டே கடவுச்சொற்கள் உருவாக்குகிறார்கள். அதாவது தங்களது தனிப்பட்ட தகவல்களை கொண்டு இலகுவாக ஞாபகப்படுத்தும் கடவுச்சொற்களை உருவாக்குகிறார்கள். இது மிகவும் தவறான முறையாகும். இதன் மூலம் தாக்குதல் நடத்துபவர்கள் உங்கள் கடவுச்சொற்களை எளிதாக ஊகிக்க முடியும்.

எனவே இது போன்ற வார்த்தைகளை உங்கள் கடவுச்சொல்லாக பயன்படுத்துவதை தவிர்க்க வேண்டும்.

கடவுச்சொல் தாக்குதல்கள்

கடவுச்சொல் தாக்குதல்களில் பல்வேறு வகைகள் உள்ளன.

அகராதி தாக்குதல்கள் (Dictionary attacks)

மீண்டும் மீண்டும் சோதனைகள் செய்வதன் (trial and error) மூலம் கடவுச்சொற்களை ஊகித்தல் (பெரும்பாலும் தன்னியக்கமாக) நடைபெறுகிறது. நீங்கள் தொடர்பின்றி எழுந்தமானமாக எடுக்கும் எழுத்துக்களை உபயோகிப்பதன் வாயிலாகவோ அல்லது வேண்டுமென்றே எழுத்துப்பிழையுடன் கடவுச்சொற்களை உருவாக்குவதன் மூலமோ இதனை தவிர்க்க முடியும்.

Brute-force தாக்குதல்கள்

ஏற்கனவே வழங்கப்பட்ட கடவுச்சொற்களுக்கான அளவுகளை அடிப்படையாக கொண்டு பலவேறுபட்ட வரிசைமாற்றங்களை செய்வதன் மூலம் சரியான கடவுச்சொல்லை கண்டுபிடித்தல் இதுவாகும். இதை தவிர்ப்பதற்கு நீங்கள் கடவுச்சொல்லின் நீளத்தை அதிகரிப்பதோடு குறியீடுகளையும் கடவுசொல்லினுள் பயன்படுத்தலாம்.

சமூக பொறியியல் தாக்குதல்கள் (Social engineering attacks)

சமூக திறன்களை பயன்படுத்தி மக்களை நம்பச் செய்து பெறுமதி மிக்க தகவல்களை தாக்குபவருக்கு அளிக்க செய்யும் செயன்முறை சமூக பொறியியல் எனப்படும். இது உங்கள் கடவுச்சொற்களை தாக்குவதற்கு பயன்படும் ஒரு வகையான நவீன உத்தி ஆகும். பாதுகாப்பான முறையில் இணையத்தை பயன்படுத்துதல் இந்த தாக்குதல்களை தவிர்க்க சிறந்த வழியாகும்.

ஒரு வலுவான கடவுச்சொல்லை உருவாக்க சில குறிப்புகள்:-

- ஒரு வார்த்தை அல்லது ஒரு சொற்றொடரை பயன்படுத்தி அதை நினைவில் வைத்திருக்க ஒரு தந்திரத்தை பயன்படுத்துதலே கடவுச்சொல்லொன்றை உருவாக்க சிறந்த வழி.

  உதாரணமாக:

  [N]aangal [e]llam [1]ankavin [n]alla [p]illaigal என்பதை பின்வருமாறு பயன்படுத்தலாம்.

  NE1nP@
- பெரிய மற்றும் சிறிய எழுத்துக்களை கலத்தல்
- சிறப்பு எழுத்துக்களை பயன்படுத்தல் (a-z) , (,."?),(!@$%^&*#), (0-9)
- அர்த்தமற்றதாக கடவுச்சொற்களை உருவாக்குதல்.
- நீளமான கடவுச்சொற்களை உருவாக்கல் (குறைந்தது 8 எழுத்துக்கள்)
- வெவ்வேறு கணக்குகளுக்கு வெவ்வேறு கடவுச்சொற்களை பயன்படுத்தல்
- கூடுதல் அடுக்கு பாதுகாப்பை பயன்படுத்தல் - இரண்டு காரணி சரிபார்ப்பு (two factor verification) (ஜிமெயில் , முகப்புத்தகம்)

நீங்கள் உங்கள் கடவுச்சொல்லை எவ்வாறு பாதுகாப்பீர்?

ஒரு வலுவான கடவுச்சொல்லை தேர்ந்தெடுத்ததன் பின் அதை பாதுகாப்பதும் உங்கள் கடமை ஆகும். உங்கள் கடவுச்சொல்லை மற்றவர்களுக்கு வெளிப்படுத்தவோ அல்லது கிடைக்கும்படியோ செய்யாதீர்கள்.

மேலும் உங்கள் கடவுச்சொற்களை துண்டுகளில் எழுதி உங்கள் கணினிகளிற்கு அருகில் வைக்காதீர்கள். இது மற்றயவர்கள் உங்கள் கணக்கிற்குள் இலகுவாக நுழைய ஏதுவாக அமைந்து விடும். மற்றையவர்களுக்கு உங்கள் கடவுச்சொற்களை வெளிப்படுத்த வேண்டாம். அத்துடன் தொலைபேசி அழைப்புகள், மின்னஞ்சல்கள் மூலமாக உங்கள் கடவுச்சொற்களை பெற முயற்சி செய்யும் நபர்களை பற்றி எச்சரிக்கையாக இருக்க வேண்டும்.

அணுகல் முறைகளை தவிர்த்து எப்பொழுதும் மேம்பட்ட உறுதிப்படுத்தல் முறைகளை உங்கள் இணைய சேவை வழங்குனரிடமிருந்து (ISP) கேட்டு பெற்று கொள்ளுங்கள். ”கேபரோஸ்” (Kerberos) , பொது திறவுகோல் குறியாக்கம்(public key encryption) போன்ற குறியாக்க நெறிமுறைகள் பயன்படுத்த முயற்சி செய்யுங்கள்.

பெரும்பாலான கணினி நிரல்கள் உள்நுழைவு கட்டமைப்புக்கள் கடவுச்சொல்லை ஞாபகப்படுத்தும் (Remember Password) வசதியை வழங்குகின்றன. ஆனால் இந்த திட்டங்களின் பாதுகாப்பு வெவ்வேறு இடங்களைப் பொறுத்து வேறுபடுகிறது. நீங்கள் நூலகத்திலுள்ள கணினியையோ அல்லது ,இணையசேவை நிலையங்களிலோ (Internet Café) அல்லது உங்களது அலுவலக கணினியையோ பயன்படுத்தி உள்நுழைவீராயின் அந்த

இடத்தை விட்டு செல்லும் போது ஒழுங்காக உங்கள் கணக்கிலிருந்து வெளியேறி (log off) விட்டீரா என உறுதிப்படுத்தவும்.

இணையத்தை பயன்படுத்தும் போது உங்களை பாதுகாத்து கொள்வது உங்கள் கடமையாகும்.
உங்கள் கடவுச்சொல் உங்கள் வீட்டினது திறவுகோல் போன்றது. எனவே அதை ஒழுங்காக கவனியுங்கள்/பயன்படுத்துங்கள்.

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