அலகு V கணிப்பொறி நன்னெறி மற்றும் இணையப் பாதுகாப்பு

பாடம் 17

கணிப்பொறி நன்னெறி மற்றும் இணையப் பாதுகாப்பு

கற்றலின் நோக்கங்கள் :

இந்த பாடத்தை கற்றபின் மாணவர்கள்:

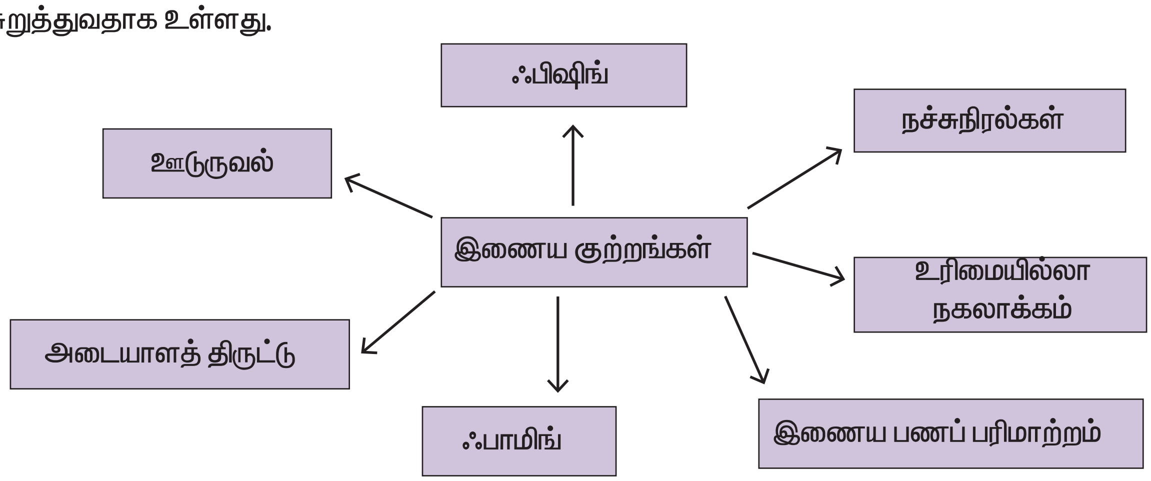
- இணைய குற்றங்கள் பற்றி அறிந்து கொள்வார்கள்.
- இணைய உலகத்தில் இணையப் பாதுகாப்பு பற்றிய வழி காட்டுதல்கள் மற்றும் அவற்றின் தேவைகள் பற்றி அறிந்துக் கொள்ளுவார்கள்.
- இணையப் பாதுகாப்பு பற்றிய சிக்கல்கள் பற்றி தெரிந்துக்கொள்வார்கள்.
- பிராக்ஸி சேவையகம் மற்றும் பயர்வால் செயல்பாடுகள் பற்றி அறிந்துக்கொள்வார்கள்.
- மறையாக்கம் மற்றும் குறியாக்கத்தின் அடிப்படை பற்றி கற்றுக்கொள்வார்கள்.
- தகவல் தொழில்நுட்ப சட்டங்கள், விதிகள், செயல்படுத்துதல் பற்றி அறிந்துக்கொள்வார்கள்.

17.1 அறிமுகம்

இணையம் என்பது எளிதாக தொடர்பு கொள்ளக்கூடிய மற்றும் அனைவறாலும் பயன்படுத்தக்கூடிய சாதனமாக உள்ளது. தகவல் தொழில்நுட்பம் என்பது கணிப்பொறிகள், கைப்பேசிகள் மற்றும் இணையம் வழியாக பரந்து விரிந்துள்ளது. தகவல் தொழில் நுட்பத்தின் நோக்கங்கள் பலவாக இருந்தாலும், அதை தவறாக பயன்படுத்தும் வாய்ப்புகள் உள்ளன.

கணிப்பொறி அமைப்பு என்பது பொதுவாக பாதிக்கப்பட கூடியது. அது தனிமனிதனின் அல்லது தொழில்களில், தினசரி வாழ்க்கையில் முக்கியப் பங்கு வகிக்கிறது. மதிப்பு மிக்க தரவுகளை தவறாக பயன்படுத்துவரின் கைகளில் கிடைத்து விடாமல், சிறப்பு பாதுகாப்பு கொடுத்து பாதுகாக்க வேண்டும். ஆகவே, தரவுகள் பாதுகாக்கப்பட வேண்டும்.

இணைய குற்றங்கள் என்பது கணிப்பொறியிலும், வலைப்பின்னல்களிலும், ஈடுபடுத்தப்படுகிறது. இது வளர்ந்து வரும் சமூகத்தின் மீது குற்றவாளிகள், பொறுப்பற்ற தனிமனிதனால் வலைதளத்தை பயன்படுத்தி தாக்குதல்கள் ஏற்படலாம். இது முக்கிய சவாலாக தகவல் தொழில்நுட்பம் பயன்படுத்துவோர் மீது உள்ளது. இணைய குற்றம், நேர்மை, பாதுகாப்பு மற்றும் வணிக அமைப்பின் வளர்ச்சியின் மீது அச்சுறுத்துவதாக உள்ளது.



படம் 17.1 பல வகையான இணைய குற்றங்கள்

நன்னெறி (ETHICS)

நன்னெறி என்பதன் அர்த்தம் **"எது தவறு மற்றும் எது சரி"** இது கணிப்பொறி யார் பயன்படுத்துகிறார்களோ, அவர்களின் தார்மீக கொள்கையின் தொகுப்பு ஆகும். ஒவ்வொரு தனிமதனிதரும் சரியான நெறிமுறை, தர்மீகத்தை பின்பற்றுவதைப் பற்றி அறிந்துக் கொள்வதே **நன்னெறி** ஆகும்.

அறநெறி என்பது சமூகத்தில் (Morals) உள்ள நல்லவை, கெட்டவைகளை ஏற்று நடப்பது ஆகும். இன்றைய இணைய உலகில் சில தர நிலைகள் உள்ளன. அவை

- திருட்டு மென்பொருளை பயன்படுத்தாமல் இருப்பது.
- அடுத்த பயனரின் கணக்கை அனுமதியின்றி பயன்படுத்தாமல் இருப்பது.
- அடுத்தவரின் கடவுச்சொல்லை திருடாமல் இருப்பது.
- ஊடுருவல் செய்யாமல் இருப்பது.

கணிப்பொறியின் நன்னெறியின் முக்கிய பிரச்சினைகள், இணைய சேவை பயன்படுத்துவோரின் தனிப்பட்ட தகவல்கள், பதிப்புரிமம் பெற்ற தரவை வெளியிடுதல். உரிமம் பெறாமல் இலக்கமுறையிலுள்ள தகவல்களை வெளியிடுதல் மற்றும் இணையத்தளத்துடன் ஊடாகுதல், மென்பொருள் மற்றும் தொடர்புடைய சேவைகள்.

கணிப்பொறி நன்னெறி (COMPUTER ETHICS)

இணையத்தின் உதவியால் உலகமானது உலக கிராமமாக தற்போது உள்ளது. தனிமனிதன் மற்றும் பல்வேறு நிறுவனங்கள் மேலும் தொழிற்நிறுவனங்கள் இணையத்தின் உதவியால் பிரபலமாகி உள்ளது என்பதை இணையதளம் நிருபித்துள்ளது. மின்வணிகம், தொழில்களில் மிகவும் பிரபலமாகியுள்ளது, ஏனென்றால் இது பல்வேறு தரப்பிலான நுகர்வோரை அணுக மற்ற வழிகளை விட வேகமாக பயன்படுகிறது.

கணிப்பெறி நன்னெறி நெறிமுறைகள் செயல்முறை, மதிப்புகள் மற்றும் நுகர்வோர் கணினி தொழிற்நுட்பத்தின் செயல்முறையை நிர்வகிக்கும் நடைமுறைகள் ஆகியவற்றைக் கொண்டுள்ளன. அதனுடன் தொடர்புடைய துறைகளில் எந்த தனிநபரின் ஒழுக்க நெறிகளும் நம்பிக்கையும் பாதிக்கப்படுவதோ அல்லது மீறாமல் செயல்படுகிறது..

நன்னெறியின் வழிகாட்டுதல்கள் (GUIDELINES OF ETHICS)

பொதுவாக, பின்வரும் வழிகாட்டுதல்கள் கணிப்பொறி பயன்படுத்துவர்கள் கவனத்தில் கொள்ள வேண்டும்.

1. நேர்மை **(Honesty)** : இணையத்தை பயன்படுத்தும் பயனர் உண்மையுள்ளவராக இருத்தல்.
2. நம்பகத்தன்மை **(Confidentiality)**: பயனர் அங்கீகரிக்கப்படாதவர்களிடம் முக்கிய தகவல்களை பரிமாற்றம் செய்யாமல் இருத்தல்.
3. மரியாதை **(Respect)** : மற்ற பயனருக்கு உள்ள தனி உரிமைக்கு உரிய மரியாதையை ஒவ்வொரு பயனரும் கொடுத்தல்.
4. தொழில்முறை **(Professionalism)** : தொழில்முறையில் ஒவ்வொரு பயனரும் தொழில் முறை நடத்தையுடன் இருத்தல்.
5. பயனர் கணிப்பொறி பயன்பாட்டின்போது சைபர் சட்டத்திற்கு கணடிப்பாக கீழ்படிதல் வேண்டும்.
6. பொறுப்பு **(Responsibility)** : ஒவ்வொரு பயனர் அவர்களின், ஒவ்வொரு செயலுக்கும் உடைமையாளராக பொறுப் பேற்றுக் கொள்ளுதல்.

உங்களுக்குத் தெரியுமா?

நன்னெறி என்பது அறநெறி கோட்பாடுகின் தொகுப்பாகும். அதுவே சமூகத்தில் ஒரு தனி மனிதனின் நடத்தையை கையாளுகின்றது. மேலும் கணிப்பொறி பயன்படுத்தும் பயனரை கட்டுப்படுத்துகிறது..

Chapter 17.indd 277 4/11/2020 11:50:40 AM

17.2 நன்னெறியின் பிரச்சினைகள் (ETHICAL ISSUES)

நன்னெறி பிரச்சினை என்பது ஒரு பிரச்சினை அல்லது தனி மனிதனுக்கோ அல்லது நிறுவனத்திற்கோ ஏற்படும், போது எது சரி (நன்னெறி) அல்லது தவறு (நன்னெறி அல்லாதது) இவற்றின் ஒன்றை தேர்வு செய்யும் முறை ஆகும். இந்த பிரச்சினை ஆனது தீர்க்கப்பட்டு சமூகத்தில் ஒரு நேர்மறையான அணுகுமுறையை கொண்டுவரவேண்டும். சில பொதுவான நன்னெறி பிரச்சினைகள் கீழே பட்டியலிடப்பட்டுள்ளது.

- சைபர் குற்றம் (cyber crime)
- மென்பொருள் உரிமையில்லா நகலாக்கம் (software piracy)
- அங்கீகரிக்கப்படாத அணுகுதல் (un Authorized access)
- ஹேக்கிங் (Hacking)
- கணிப்பொறியை பயன்படுத்தி மோசடி செய்தல் (Use of computers to commit fraud)
- நச்சு நிரல்(Virus) மூலம் நாசவேலை
- கணிப்பொறி மூலம் தவறான உரிமை கோருதல்.

இணைய குற்றம் (Cyber Crime)

சைபர் குற்றம் என்பது அறிவுசார் வெள்ளைக்காலர் குற்றமாகும். இந்த குற்றங்களை செய்வோர் பொதுவாக கணிப்பொறியை திறன்பட இயக்குபவராக இருப்பார்கள்.

உதாரணமாக – சட்ட விரோத பண பரிவர்த்தனை இணையத்தின் வழியாக நடைபெறுவதை உதாரணமாக கூறலாம். கணிப்பொறி குற்றங்களில் சில உதாரணமாக கொடுக்கப்பட்டுள்ளது.

அட்டவணை 17.1

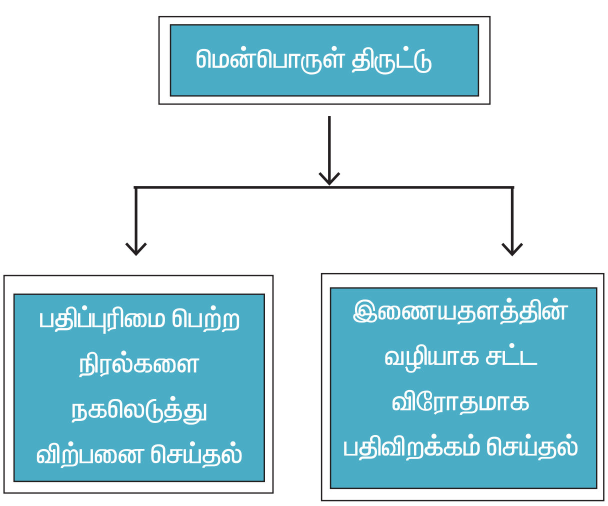
குற்றம்	செயல்பாடுகள்
சைபர் தீவிரவாதம் (Cyber terrorism)	ஒரு நபரையோ அல்லது வணிகத்தையோ திருடுதல், மிரட்டுதல் மற்றும் அச்சுறுத்தலாகும்
இணையத் தொந்தரவு (Cyber stalking)	இணையத்தின் மூலம் நெருக்கடி கொடுத்தல்
தீம்பொருள் (Malware)	இணையவழி தொந்தரவு பல்வேறு செயல்களான திருடுதல், மறையாக்கம் அல்லது முக்கியமான தரவுகளை நீக்கம் செய்தல், எச்சரிக்கை அல்லது கணிப்பொறி செயல்பாடுகளை நடத்துதல், செயல்பாடுகளை பயனர் அனுமதி இல்லாமல் கண்காணித்தல்.
சேவை தாக்குதல்களின் மறுப்பு (Denial of service attack)	போலி கோரிக்கைகள் மூலம் அளவுக்கதிகமான கணிப்பொறி அமைப்பினால் சாதாரண சட்டவிரோத கோரிக்கைகள் பணியாற்ற இயலாத நிலை.
மோசடி (Fraud)	தரவுகளை தவறாக கையாளுதல், உதாரணமாக வங்கி பதிவுகளை மாற்றுவதன் மூலம் அங்கீகாரமில்லாத வங்கி கணக்கிற்கு பண பரிவர்த்தனையில் மோசடி செய்தல்.
அரண் உடைத்தல் (Harvesting)	சட்டவிரோதமாக அடுத்த பயனரின் பயனர் பெயர் மற்றும் கடவுச் சொல்லை சேகரித்து, பயனரின் கணக்குகளில் நுழைந்து பயனடைதல்.
அடையாளத் திருட்டு (Identity theft)	நிதி ஆதாயத்திற்காக, தனி நபரின் அடையாளத்தை குற்றவாளிகள் பயன்படுத்துதல்.

அறிவுசார் சொத்து திருட்டு (Intellectual property theft)	ஒரு நிறுவனத்தால், தனி நபரால் உருவாக்கப்பட்ட நடைமுறை அல்லது கருத்தியல் தகவலை திருடுதல்
சலாமி ஸ்லைசிங் (Salami slicing)	இணைய பண பரிவர்த்தனையில் சிறிய அளவாக பணம் திருடுதல்.
ஊழல் (Scam)	உண்மை இல்லாத ஒன்றை, மக்களை நம்ப வைத்து ஏமாற்றுவது.
ஏமாற்றுதல் (Spoofing)	அறியப்படாத மூலத்திலிருந்து பெறுபவர் அறியப்பட்ட ஆதாரத்தை அனுப்பி தீங்கிழைக்கும் நடைமுறையாகும்..
ஸ்பேம் (Spam)	தேவையற்ற மின்னஞ்சலை அதிக எண்ணிக்கையில் இணைய தள பயனர்களுக்கு அனுப்புதல்.

மென்பொருள் திருட்டு (SOFTWARE PIRACY)

மென்பொருள் திருட்டு என்பது ஒரு தனிப்பட்ட அல்லது ஒரு நிறுவனத்தால் முதலில் உருவாக்கப்பட்ட மென்பொருளை பதிப்புரிமை பெறாமல், சட்ட விரோதமாக குறியீடுகள், தகவல்கள், நிரல்கள் மற்றும் பிற தகவல்களை திருடுதல். அங்கீகாரம் இல்லாமல், நகல்களின் பிரதிகளை உருவாக்கி இந்த தரவை சொந்த நலனுக்காக, அல்லது வணிக இலாபத்திற்காக பயன்படுத்துவது ஆகும்.

எளிமையான கூறவேண்டுமெனில் மென்பொருள் திருட்டு என்பது **"மென்பொருள்களின் அங்கீகரிக்கப்படாத நகல்"** ஆகும்.



படம் 17.2- மென்பொருள் திருட்டின் விளக்கப்படம்

பெரும்பாலான மென்பொருள்கள் ஒரே கணிப்பொறியில் மட்டுமே பயன்படுத்த அனுமதிக்கப்படுகின்றன அல்லது ஒரே நேரத்தில் ஒரு பயனரால் மட்டுமே பயன்படுத்தப்படுகின்றன. ஒரு பயனர் மென்பொருளை வாங்கும் போது அதன் மென்பொருள் உரிமம் பெற்ற பயனராகிறார். காப்புரிமை பயன்பாட்டிற்கான நகல்களில் பிரதிகள் தயாரிக்க அனுமதிக்கப்படுவர். நகல்களை மற்றொருவருக்கு விநியோகம் செய்வது சட்ட விரோதமானது.

மென்பொருள் திருட்டிற்கு முற்றிலும் மாறுபட்ட அணுகுமுறை **பகிர்மான மென்பொருள்** என அழைக்கப்படுகின்றன. நகலெடுப்பதில் இருந்து மக்களை தடுக்க முயற்சிப்பதால் பயனில்லை. மாறாக மக்களுக்கு நேர்மையை உணரச்செய்யலாம்.

நிரலை உருவாக்கியவர்க்கு நேரடியாக ஒரு பதிவு கட்டணத்தை செலுத்தி, பயனர்களும், சக ஊழியர்களும், நிரல்களை நகலெடுக்க பகிர்மான மென்பொருள் ஊக்கப்படுத்தப்படுகிறது. சட்ட விரோதமாக பொதுமக்களுக்கு கிடைக்ககூடிய வணிக நிரல்கள் பெரும்பாலும் **வார்ஸ்கள் (warez)**என்று அழைக்கப்படுகின்றன.

அங்கீகரிக்கப்படாத அனுமதி

அங்கீகாரமற்ற அணுகல் என்பது ஒரு வலைதளம், நிரல், சேவையகம் அல்லது பிற முறைமைக்கான அணுகல் முறையான பயனர் கணக்கை மீறுவதன் மூலம் அது அங்கீகரிக்கப்படாத அணுகல் எனப்படும். எடுத்துக்காட்டாக ஒருவருடைய பயனர் கணக்கும் பெயர், கடவுச்சொல்லை பயன்படுவதையே அங்கீகரிக்கப்படாத அனுமதியாகும்.

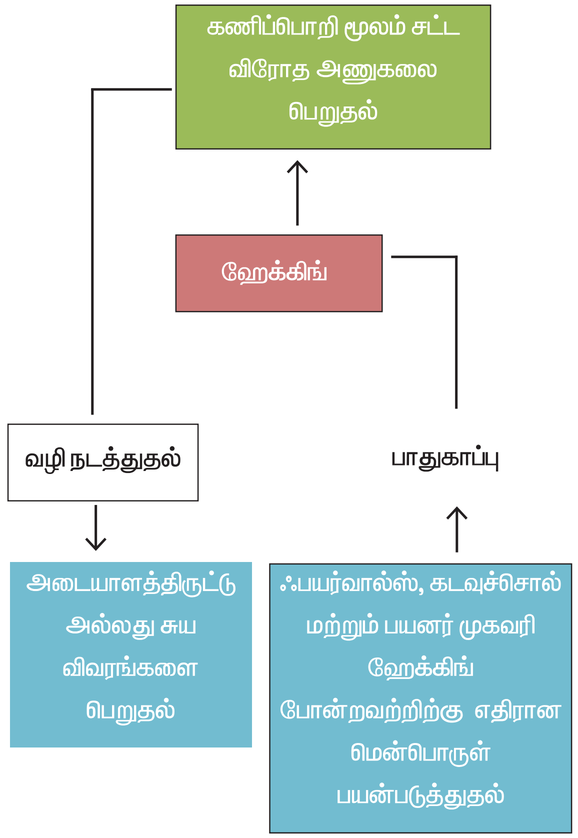
அங்கீகரிக்கப்படாத அணுகுதலை தடுக்க பயர்வால்கள், இன்ட்ருஷன் டிடெக்டிக் சிஸ்டம்ஸ்

Chapter 17.indd 279 4/11/2020 11:50:41 AM

(**Intrusion Detection Systems** - IDS), நச்சு நிரல் மற்றும் உள்ளடக்க வருடிகள் பயன்படுத்தப்படுகின்றன.

ஹேக்கிங்

ஹேக்கிங் என்பது ஒரு கணிப்பொறியின் உரிமையாளரின் அனுமதி இல்லாமல், தனிப்பட்ட தரவு அல்லது கடவுச் சொல்லை குற்றம் சார்ந்த நடவடிக்கையாகவோ அல்லது பொழுது போக்கிற்காகவோ திருடுதல். இது மேலும் கணிப்பொறி அமைப்பில் அனுமதி பெறாமல் அணுகுதலாகும். மேலும் அதிலுள்ள பொருளடக்கத்தை மாற்றுதலாகும். இதை பொழுதுபோக்கு சவாலாக செய்தால் இதை நெறிமுறை ஹேக்கிங்காகும். இத்தகைய நெறிமுறை ஹேக்கிங் மட்டுமே கட்டுப்படுத்தப்பட்ட சோதனைகள் என நடைமுறைப்படுத்தப்பட வேண்டும்.



படம் 17.3 ஹேக்கிங் வரைபடம்

கிராக்கிங்

நிரலை பதிப்பித்து அதை பயனருக்கு தேவையற்றதாக மாற்றுவது கிராக்கிங்காகும். கிராகர் (ஒரு கருப்பு தொப்பி அல்லது இருண்ட பக்க ஹேக்கர் என்று அழைக்கப்படுவர்). கணிப்பொறி அமைப்பில் சட்டவிரோதமாக தரவுகளை திருடுதல் அல்லது மாற்றம் செய்தல்.

கிராக்கர் என்பவர் மற்றொரு கணிப்பொறி கட்டமைப்பில் இணையம் மூலம் நுழைந்து அவரின் கடவுச் சொல்லை அல்லது உரிமத்தை சட்டவிரோதமாக கண்டறிந்து வேலை செய்தல்.

மென்பொருள் சிதைவு என்பது மிகவும் அடிக்கடி ஏற்படுத்தப்படும் சிதைவு வகை ஆகும். கடவுச்சொல் விரிசல் என்று மற்றொரு வகை உள்ளது. இது கடவுச் சொற்களை அழிக்கப்பயன்படுகிறது. தானியங்கு திட்ட நிரல்களை பயன்படுத்தி கடவுச் சொல் கிராக் செய்வது அல்லது கைமுறையிலும் செய்யலாம்.

கிராக்கிங் என்பது ஒரு சுவாரசியமான உண்மை, சமூக கட்டமைப்பு ஆகும். மனிதனுடைய பலவினத்தைப் பயன்படுத்தி, கடவுச் சொற்கள் மட்டும் தகவல்களை பெறும் வழியாகும். இது மென்பொருள் அல்ல தகவல்களைப் பெறுவதற்கு தொலைபேசியை பயன்படுத்தலாம். உங்கள் நண்பர்களாக இருப்பதுடன் இணைய ரிலே அரட்டை (IRC) அல்லது நல்லவராக உங்களுடன் பேசி தகவல்களை பெறலாம். மின்னஞ்சல் அவர்களுக்கு ஒரு அதிகாரபூர்வ மின்னஞ்சலாக, வங்கி அல்லது பிற அதிகார பூர்வ நிறுவனங்களின் மின்னஞ்சல் போல் தோன்றலாம்.

உங்களின் தனிப்பட்ட தகவல்களை அவர்கள் கண்டுபிடித்து கடவுச்சொல்லை யூகிக்க முயற்சி செய்கிறார்கள். தனிப்பட்ட நன்மைக்காக அவர்களே கண்டுபிடித்து அவற்றை சுரண்டுவதில் உள்ள பாதிப்புகள் பற்றி அறிந்து கொள்ளலாம்.

17.3 இணையப் பாதுகாப்பு மற்றும் அச்சுறுத்தல்கள்

ஒரு கணிப்பொறிக்கு கணிசமான சேதத்தை ஏற்படுத்தவோ அல்லது ஒரு நபரிடமிருந்து அல்லது ஒரு நிறுவனத்திடமிருந்து முக்கியத் தகவல்களை திருடுவதாகவோ, இணைய தாக்குதல்கள் முதன்மையாக தொடங்கப்பட்டது. இணையப் பாதுகாப்பு என்பது பல்வேறு தொழில்நுட்பங்கள் செயல்முறைகள் மற்றும் நடவடிக்கைகள் ஆகியவற்றின் தொகுப்பாகும். இது இணைய தாக்குதல்களின் ஆபத்தை குறைக்கும் மற்றும் நிறுவனங்கள் மற்றும் தனிநபர்கள் பாதுகாக்கும் கணிப்பொறி சார்ந்த அச்சுறுத்தல்களில் இருந்து பாதுகாக்கும்.

Chapter 17.indd 280 4/11/2020 11:50:41 AM

இணையத் தாக்குதல்களின் வகைகள்

தீம் பொருள் மென்பொருள் சட்ட விரோதமான அணுகல் மற்றும் சேதம் விளைவிக்கும் வகையில் வடிவமைக்கப்பட்ட ஒரு வகை மென்பொருள் ஆகும். பல வகையான இணைய தாக்குதல்கள் மற்றும் அவற்றின் செயல்பாடுகள் ஆகியவை அட்டவணை 17.2 ல் கொடுக்கப்பட்டுள்ளன.

அட்டவணை 17.2 – இணையத் தாக்குதல்கள் மற்றும் செயல்பாடுகள்

வ.எண்	இணையத் தாக்குதல்கள்	செயல்பாடுகள்
1.	நச்சு நிரல்	ஒரு நச்சு நிரல் என்பது கணிப்பொறி குறியீட்டின் ஒரு சிறிய பகுதி ஆகும். அது தன்னை மீண்டும் மீண்டும் ஒரு கணிப்பொறியில் இருந்து மற்றொரு கணிப்பொறிக்கு கோப்புடன் இணைக்கும் வகையில் பரவுகிறது. பொதுவான நச்சு நிரல் ட்ரோஜன் ஆகும். ஒரு ட்ரோஜன் நச்சு நிரல் என்பது ஒரு செயல்பாடு. எடுத்துக்காட்டாக – நச்சு நிரல் நீக்கம் ஒரு எடுத்துக்காட்டாக கூறலாம். உண்மையில் நச்சு நிரல் செயல்படுத்தப்படும் போது தீங்கிழைக்கும் செயல்களை செய்கிறது.
2.	வார்ம்ஸ்	வார்ம்ஸ் என்பது சுயமாக திரும்ப திரும்ப வந்து இணைத்துக் கொள்ளும். இதை செய்ய நிரல்கள் தேவை இல்லை. வார்ம்ஸ் தொடர்ந்து பாதிப்புக்குள்ளாகி பலவீனங்களை கண்டுபிடித்து வார்ம்ஸின் நிரலாலருக்கு தெரிவிக்கிறது.
3.	ஸ்பைவேர்	கணிப்பொறியின் இணைப்புக்களை திறக்கும் போது தானாகவே கணிப்பொறியில் நிறுவப்படலாம். இணைப்புகளில் கிளிக் செய்யும் போதும் பாதிக்கப்பட்ட மென்பொருளை பதிவிறக்கம் செய்வதன் மூலமும் ஸ்பைவேர் நிறுவப்படலாம்..
4.	ரேன்சம்வேர்	ஒரு கணிப்பொறியில் இணைய தாக்குதல்களில் தொடங்குவதற்கு பிறகு பணம் கோரி தீங்கு இழைக்கத் திட்டமிடுதல். இந்த தீம்பொருள் குற்றவாளிகளுக்கிடையே பெருகிய முறையில் பிரபலமடைந்து ஒவ்வொரு வருடமும் நிறுவனங்களுக்கு மில்லியன் கணக்கான செலவுகளை ஏற்படுத்துகிறது..

பாதுகாப்பின்மை (threats)

சமீபத்திய வருடங்களாக பாதுகாப்பு அமைப்புகளில் உள்ள பலவீனங்கள் காரணமாக தனிநபர்கள் மற்றும் நிறுவனங்கள் பெரும்பாலான பிரச்சினைகளை எதிர்கொள்கிறது. பல்வேறு வகையான சைபர் பாதுபாப்பின்மை அச்சுறுத்தல்கள் கீழே வகைப்படுத்தப்பட்டுள்ளன.

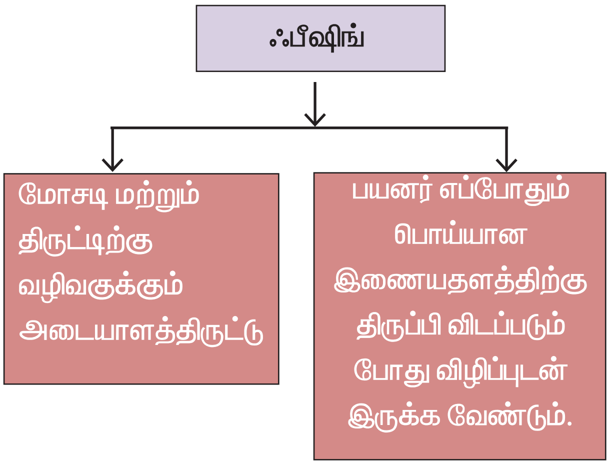
சமூக கட்டமைப்பு

சமூக கட்டமைப்பு ஒரு நபரின் பலவீனத்தை தவறாக பயன்படுத்தி தீங்கிழைக்கும் இணைப்புகளை கிளிக் செய்வதன் மூலமும் அல்லது நுணுக்கங்கள் மூலம் கணிப்பொறியை அணுகுவதாலும் பெறப்படுகிறது.ஃபிஷிங் மற்றும் ஃபார்மிங் சமூக கட்டமைப்புகளுக்கு உதாரணங்கள் ஆகும்.

ஃபீஷிங்

ஃபீஷிங் என்பது கணிப்பொறி குற்றத்தின் ஒரு வகை ஆகும். கடவுச்சொல் மற்றும் கிரெடிட் கார்டு எண்கள் உள்ளீட்ட பயனர் தரவை திருடுவதற்கு பயன்படுத்தப்படும். ஒரு மின்னஞ்சல் அல்லது ஒரு உடனடி உரைச் செய்திப்பெட்டியை திறக்கும் போது அது பாதிப்புக்குள்ளாகி தீங்கிழைக்கக்கூடிய இணைப்புகள் அல்லது இணைப்புகளை விநியோகிக்க ஃபீஷிங் பயன்படுகிறது. ஒரு பாதிக்கப்பட்டவரிடமிருந்து முக்கிய உள்நுழைவு சான்றுகளை பிரித்தெடுத்தல் உட்பட பலவிதமான செயல்பாடுகளை செய்ய முடியும்.

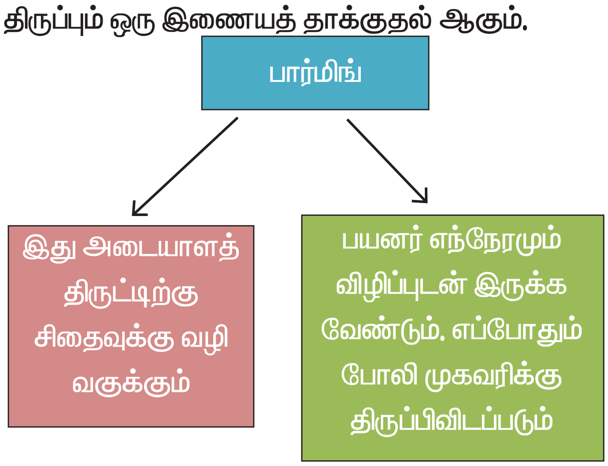
Chapter 17.indd 281 4/11/2020 11:50:41 AM



படம் 17.4 ஃபீஷிங் வரைபடம்

பார்மிங் (Pharming)

பார்மிங் என்பது ஒரு தனிப்பட்ட கணிப்பொறியின் அல்லது சேவையகத்தின் தீங்கிழைக்கும் குறியீடு உள்ள மோசடியான ஒரு நடைமுறை ஆகும். பயனரின் அனுமதி இல்லாமல் தவறான வலை தளங்களை தவறாக வழி நடத்துகிறது. பயனரை மோசடி செய்ய ஷேக்கர்கள் முயற்சி செய்து வலைதளத்தின் போக்கை திசை திருப்பும் ஒரு இணையத் தாக்குதல் ஆகும்.

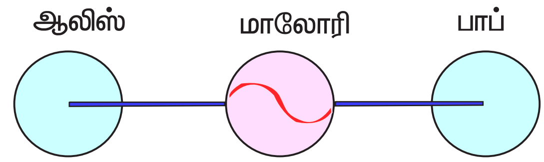


படம் 17.5 பார்மிங் வரைபடம்

ஒரு நபர் மீது தாக்குதல் (Man In The Middle (MITM)) :

ஒரு நபர் மீது தாக்குதல் (MITM மற்றும்) என்பது இரகசியமாக தொடர்பு ஏற்படுத்தி தாக்குதல்,மேலும்ஒருவரோடுஒருவர் நேரிடையாக தொடர்பு கொள்வதாக நம்புகிற இரு கட்சிகளிடையே தொடர்பை மாற்றியமைத்து, தாக்குதல் தொடுப்பது ஆகும்.

எடுத்துக்காட்டு பாப் உடன் தொடர்பு கொள்ள ஆலிஸ் விரும்புகிறார் என கருதினால் இடையில் பல்வேறு உரையாடலை இடைமறித்து, பாப் தவறான செய்தி பெறுவது போல் செய்வது ஆகும்.



படம் 17.6 – ஒரு நபர் மீது தாக்குதல்

குக்கிகள் (Cookies)

ஒரு குக்கி (இணைய குக்கி, HTTP குக்கி, வெற்று குக்கி, உலவி குக்கி அல்லது சாதாரண குக்கி) என்பது வலை தளத்திலிருந்து அனுப்பப்பட்ட ஒரு சிறிய துண்டு தரவு மற்றும் பயனரின் இணையமானது அனைத்து வலை தளங்களின் ஒரு இணைய தளத்தில் இணைய தள அங்காடியில் சேர்க்கப்பட்ட பொருட்கள் போன்றவை ஆகும். பயனரின் பயன்பாட்டால் பொத்தானை கிளிக் செய்து உள் நுழைதல் அல்லது பதிவு செய்தல், வலைதளங்களுக்கான நம்பகமான கருவியாக வடிவமைக்கப்பட்டுள்ளது. பயனரின் பழைய பயர்வால், முகவரிகள், கடவுச் சொற்கள் மற்றும் கடன் அட்டை எண்கள் போன்ற பிரபலங்கள் உள்ளிட்ட பயனர் தன்னிச்சையின் தகவல்களை நினைவில் வைத்து பயன்படுத்தலாம். குக்கி தரவு இடைமறிக்கப்பட்டால் பாதுகாப்பு கண்ணோட்டத்தில் இருந்து, பயனர் குக்கி தகவலை அறிந்து. தவறாக பயன்படுத்தவும் வாய்ப்பு உள்ளது. பின்வரும் காரணங்களுக்காக வலைதளங்கள் பொதுவாக குக்கிகளை பயன்படுத்துகின்றன.

- இணைய தளத்திற்கு சென்று பார்த்தவர்கள் பற்றிய விவரங்களை சேகரிக்க, இந்த இணைய தளத்தை பெரும்பாலும், எத்தனை பார்வையாளர்கள் பார்வையிட்டனர் எவ்வளவு நேரம் பார்வையிட்டார்கள் என்பதையும் கண்காணிக்கலாம்.
- இது வலை தளத்தின் பயனரின் அனுபவத்தை தனிப்பயனாக்க உதவுகிறது.
- குக்கிகள் பயனர் பற்றியத் தனிப்பட்ட தகவல்களை சேமித்து வைக்க உதவும்.
- இதன் மூலம் ஒரு பயனர்கள் தளத்திற்கு திரும்பும் போது அதிக அனுபவங்கள் பெறப்படுகின்றன.

இணைய தளத்தில் எப்போதாவது திரும்பி சென்றால், உங்கள் பெயர் மர்மமாக திரையில் தோன்றும், முந்தைய வருகையின் காரணமாக உங்கள் பெயரை தளத்தில் கொடுத்து இருந்தீர்கள் என்றால் அதே குக்கியில் சேமிக்கப்பட்டுள்ளதற்கு ஒரு சிறந்த உதாரணம்.

Chapter 17.indd 282
4/11/2020 11:50:41 AM

இணையதள அங்காடி தளத்தில், ஏற்கனவே பொருட்கள் வாங்கியதன் அடிப்படையில் பயனர்களுக்கு பரிந்துரைக்கும் வழியாகும். விளம்பரங்களை கண்காணிக்கவும் குக்கிகள் பயன்படுத்துகின்றன. குக்கிகள் கணிப்பொறியில் தீமை செய்யவில்லை அவை எந்த நேரத்திலும் நீக்கப்பட கூடிய உரை கோப்புகள் ஆகும்.

நச்சுநிரல்கள் பரப்புவதற்கு குக்கிகளை பயன்படுத்த இயலாது. மேலும், அவை உங்கள் இயக்கிகளை அணுக இயலாது. குக்கியின் அம்சமானது வெளிப்படையாக உங்கள் உலவியில் நிறுத்தப்படாவிட்டால் கடன் அட்டை தகவலை உள்ளடக்கிய ஒரு நபரின் தனிப்பட்ட தகவல்கள் வலைத் தளத்திற்கு வழங்கப்படும்.

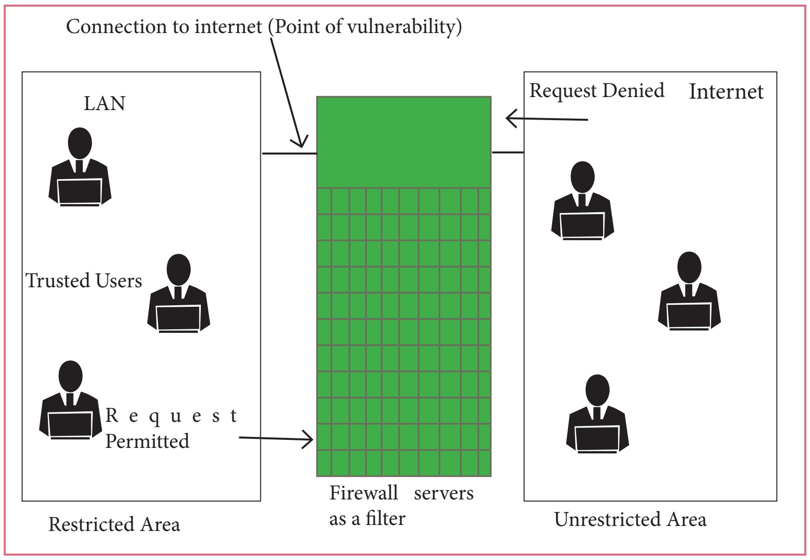
இந்த வகையில் தான் குக்கிகள் பாதுகாப்பை அச்சுறுத்துகின்றன.

ஃபயர்வால் மற்றும் மறைமுக (proxy) சேவையகங்கள்

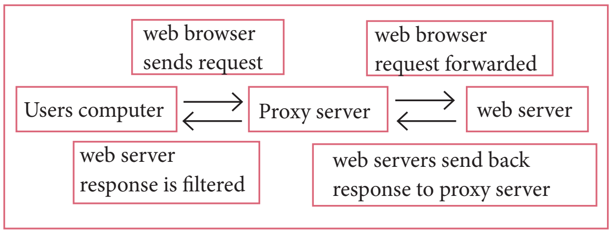
ஃபயர்வால் மற்றும் பதிலாள் சேவையகங்கள் என்பது கணிப்பொறி வலையமைப்பு பாதுகாப்பு அடிப்படை அமைப்பாகும். பாதுகாப்பு அடிப்படையில் உள்வரும் மற்றும் வெளிச் செல்லும் வலையமைப்பு போக்குவரத்து போன்றவற்றை கண்காணித்து கட்டுப்படுத்துகிறது. ஃபயர்வால் பொதுவாக நம்பகமாக உள்ள கணிப்பொறி வலைதளம் மற்றும் வலைப்பின்னலுக்கு வெளியே உள்ள கணிப்பொறிக்கும் இடையே ஒரு தடையை அமைக்கிறது. இவை இணையம் அல்லது முனையை (host) அடிப்படையாகக் கொண்டு வகைப்படுத்தப்படுகின்றன. வலையமைப்பு அடிப்படையிலான ஃபயர்வால்கள் LAN, WAN மற்றும் இணையம் ஆகியவற்றின் கணிப்பொறியில் வைக்கப்பட்டுள்ளன. முனையம் தழுவிய ஃபயர்வால்கள் வலையமைப்பு கணிப்பொறியில் இருத்தப்படுகின்றன.

ஃபயர்வால் என்பது இயங்கு தளத்தின் ஒரு பகுதியைப் போன்ற சேவையாக அல்லது பாதுகாப்பு போன்ற ஏஜென்ட் பயன்பாட்டாக இருக்கலாம். ஒவ்வொன்றிலும் நன்மைகள் மற்றும் தீமைகள் உள்ளன. இருப்பினும் ஒவ்வொன்றுக்கும் அடுக்கு பாதுகாப்பில் ஒரு பங்கு உள்ளது. தகவல் தொடர்பு ஆரம்பிக்கப்படுதல், குறுக்கீடு செய்யப்படுதல், தொடர்புநிலை கண்டுபிடிக்கப்படுதல் ஆகியவற்றைப் பொறுத்து ஃபயர்வால்களின் வகைகள் மாறுபடுகின்றன. படம் 17.7ல் ஃபயர்வால் சேவையகம் வேலை செய்யும் விதத்தை காண்பிக்கிறது.

ஒரு மறைமுக (proxy) சேவையகம், இறுதி பயனர்களுக்கும், வலை சேவையகத்திற்கும், இடையில் இடைத்தரகராக செயல்படுகின்றன. கோப்பு இணைப்பு, வலைப்பக்கம் அல்லது வேகமான வேறுபட்ட சேவையகத்திலிருந்து கிடைக்கும் பிற வளங்கள் போன்ற சில சேவைகளை பயனாளர் மறைமுக சேவையாகத் திடம் வேண்டுகிறார். பிராக்ஸி சேவையகம் கோரிக்கையை ஆராய்கிறது. நம்பகத்தன்மையை ஆராய்ந்து அதன்படி கோரிக்கை வழங்கப்படுகிறது. பிராக்ஸி சேவையகங்கள் பொதுவாக அடிக்கடி பார்வையிடும் தள முகவரிகள் அதன் தற்காலிக சேமிப்பில் மேம்பட்ட பதிலளிப்பு நேரத்திற்கு வழிவகுக்கும்.



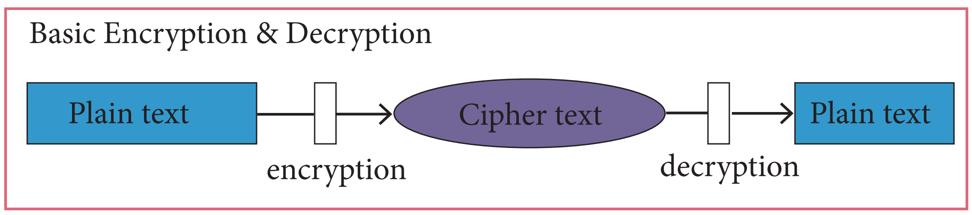
படம் 17.7 ஃபயர்வால் சேவையகம்



படம் 17.8 பிராக்ஸி சேவையகத்தின் செயல்பாட்டை படம் விளக்குகிறது.

குறியாக்கம் மற்றும் மறை குறியாக்கம்

குறியாக்கம் மற்றும் மறை குறியாக்கம் என்பது அங்கீகரிக்கப்பட்ட நபர்கள் மட்டுமே தகவலை அணுக முடியும் என்ற இரகசியத்தை உறுதிப்படுத்தும். குறியாக்கமானது எளிய உரைத் தரவு, சீரற்ற மற்றும் சிக்கனமான தரவுகளாக சிபர் உரை மாற்றும் முறை ஆகும். மறைக்குறியாக்கமானது சீரற்ற மற்றும் சிக்கனமான தரவுகளை எளிய உரைகளாக மாற்றும் தலைகீழ் முறையாகும். குறியாக்கம் மற்றும் மறைகுறியாக்கம் ஆகிய இரண்டும் குறிமுறையாக்கத்தைக் கொண்டு செய்யப்படுகிறது. குறிமுறையாக்கத்தின் திறவுகோல் என்பது குறிமுறையாக்க நெறிமுறையின் வெளியீடைக் கண்டறியும் தகவலின் ஒரு பகுதியாகும்.



படம் 17.9 குறியாக்கம் மற்றும் மறை குறியாக்கம்

குறியாக்கம் என்பது இரகசிய குறியீடுகளை பயன்படுத்தி அரசாங்கம் மற்றும் இராணுவத்தை தொடர்பு கொள்ள பயன்படுத்தும் இரகசிய மொழியாக பயன்படுகிறது. பொதுமக்கள் அமைப்புகளில் தகவலை பாதுகாக்க பயன்படுகிறது. உதாரணமாக, வலைதளம், தொலைபேசி, கம்பியில்லா நுண்ணிய தொலைபேசி, புளுடூத் மற்றும் தானியங்கி கருவிகள் போன்றவற்றில் தகவலைப் பாதுகாக்கிறது. அண்மை ஆண்டுகளில் தகவல் தொடர்பில் குறிப்பிடத்தக்க குறுக்கீடுகள் உள்ளதாக எண்ணிலடங்கா குற்றச்சாட்டுக்கள் உள்ளன.

தரவுகள் வலையமைப்புகளுக்கிடையே அனுப்பப்படும்போது வலைதள போக்குவரத்தில் அங்கீகரிக்கப்படாத பயனர்களிடமிருந்து பாதுகாப்பதற்காக குறியாக்கம் செய்யப்படவேண்டும்.

17.4 தகவல் தொழில்நுட்ப சட்டம் அறிமுகம் (Introduction to Information Technology Act)

21ஆம் நூற்றாண்டில், கணிப்பொறி, இணையதள மற்றும் ஐ.சி.டி அல்லது மின்னணு புரட்சி என்பது மனிதனின் வாழும் முறையை மாற்றி உள்ளது. இன்று காகிதத்தை அடிப்படையாகக் கொண்டு உள்ள தொடர்பு சாதனம், மின்னணு தொடர்பு சாதனமாக மாறி உள்ளது. அதன் படி நாம் பெற்றுள்ள புதிய சொற்கள் இணைய உலகம், மின்னணு பறிமாற்றம், மின்னணு வங்கி, மின்னணு வருமான வரி பிடித்தம் மற்றும் மின்னணு ஒப்பந்தம் முதலியன. இது ஒரு பக்கம் மின்னணு புரட்சி நன்மையாக இருந்தாலும், மற்றொரு பக்கம் தீமைகளும் உள்ளன. இணைய சேவை மற்றும் ஐ.சி.டி ஆகியவை குற்றவாளிகள் கைகளில், குற்றமிழைப்பதற்கு ஆயுதமாக உள்ளது.

ஆகவே, புதிய உறுப்பினர்களை கொண்ட குழு அமைக்கப்பட்டு இணைய உலகில் உள்ள இணைய குற்றங்கள் கையாளப்பட வேண்டும். எனவே, இணைய சட்டங்கள் அல்லது இணையவெளிச் சட்டங்கள் அல்லது தகவல் தொழில்நுட்ப சட்டங்கள் அல்லது இணைய சட்டங்கள் கொண்டு கையாளப்பட வேண்டும். இந்தியாவில் இணையச்சட்டம் (IT ACT 2000) 2008ல் புதுப்பிக்கப்பட்டு கணிப்பொறி குற்றங்களைத் தடுப்பதற்காக பயன்படுத்தப்படுகிறது. IT ACT 2000, EDI (Electronic Data Interchange) மற்றும் பிற மின்னணு தொடர்புகளின் வழியாக மேற்கொள்ளப்படும் பரிவர்தனைகளுக்கான சட்ட அங்கீகாரத்தை வழங்குகிறது. இந்தியாவில் குற்றம் மற்றும் மின் வணிகம் (e-commerce) ஆகியவற்றை கையாள்வதற்கு இந்தச் சட்டம் முக்கியமானதாகும். மின்வணிகம் என்பது மின்னணு தகவல் பரிமாற்றம் அல்லது மன்னணு தகவல் பதிவுசெய்தல் ஆகும்.

Chapter 17.indd 284 4/11/2020 11:50:41 AM

உங்களுக்குத் தெரியுமா?

“சைபர் சட்டம்” (cyber law) என்பது இணையபயன்பாட்டுடன் தொடர்புடைய சட்ட சிக்கல்களை தீர்க்க உதவுகிறது.

25% சைபர் குற்றங்கள் தீர்க்கப்பட்டதவையாக உள்ளன. தகவல்களைப் பாதுகாக்க பின்வருவனவற்றை கவனிக்க வேண்டும்.

1. சிக்கலான கடவுச்சொல்லை உருவாக்குவதால் தரவுகளுக்கு பாதுகாப்பை வழுங்கமுடியும்
2. இணையதளத்தை பயன்படுத்தவில்லை என்றால் இணைப்பை துண்டிக்க வேண்டும்.
3. ஸ்பேம் (spam) மின்னணு அஞ்சல் மற்றும் உங்களுக்கு அறிமுகம் இல்லாதவர்களின் மின்அஞ்சல்களை திறக்க கூடாது
4. ஆன்டி நச்சுநிரலை நிறுவி மேம்பாடு செய்து (Update) கொள்ள வேண்டும்..

உங்களுக்குத் தெரியுமா?

1. விழிப்புணர்வு என்பது பாதுகாப்பின் சிறப்பம்சம் ஆகும்
1. தகவல் பாதுகாப்பு என்பது வணிகத்தின் முக்கிய பகுதியாகும்
1. இணையத்தில் பரிவர்த்தனை செய்யும்பொழுது விரைவாக எதையும் கிளிக் செய்யகூடாது
1. கடவுச் சொல்லை யாருடனும் பகிர்ந்து கொள்ளக் கூடாது.

மதிப்பீடு

I சரியான விடையைத் தேர்ந்தெடுக்க

N2MF7Y

1. கீழ் கண்டனவற்றில் எது செயல்முறை, பயிற்சி மற்றும் மதிப்புடன் தொடர்புடையது?

   அ. உரிமையில்லா நகலாக்கம்

   ஆ. நிரல்கள்

   இ. நச்சு நிரல்கள்

   ஈ. கணிப்பொறி நன்னெறி

2. வணிக நிரல்களை பொது சட்ட விரோதமாக பயன்படுத்துவது

   அ. இலவச பொருள்

   ஆ. வேர்ஸ்

   இ. இலவச மென்பொருள்

   ஈ. மென்பொருள்

3. கீழ்கண்டவற்றுள் எது கணிப்பொறி நிரல்களின் தேவையில்லாமல் தானே பெருக்கிக் கொள்ளவும் மற்றும் இணைத்துக் கொள்ளவும் செய்யும்?

   அ. நச்சுநிரல் ஆ. வார்ம்ஸ்

   இ. ஸ்லைவேர் ஈ. ட்ரோஜன்

4. கீழ்கண்டவற்றில் எது பயனர் இணைய தளத்தை பார்வையிடுவதை கண்காணிக்கிறது?

   அ. ஸ்பைவேர் ஆ. குக்கிகள்

   இ. வார்ம்ஸ் ஈ. ட்ரோஜன்

5. கீழ்கண்டவற்றில் எது தீங்கிழைக்கும் நிரல்கள்?

   அ. வார்ம்ஸ் ஆ. ட்ரோஜன்

   இ. ஸ்பைவேர் ஈ. குக்கிகள்

6. கணிப்பொறி வலைப்பின்னல் வழியாக உள்நுழையவும், வெளியேறவும், சமிக்ஞைகளை கண்காணிக்கவும் கட்டுப்படுத்தவும் வகை செய்வது

   அ. குக்கிஸ் ஆ. நச்சுநிரல்

   இ. பயர்வால் ஈ. வார்ம்ஸ்

7. சிபர் எழுத்ததை தனி எழுத்தாக மாற்றம் செய்யும் முறை

   அ. குறியாக்கம்

   ஆ. மறை குறியாக்கம்

   இ. நச்சு நிரல்கள்

   ஈ. பிராக்ஸி சேவையகம்

8. இ- வணிகம் என்பது

   அ. மின்னணு வணிகம்

   ஆ. மின்னணு தரவு மாற்றம்

   இ. மின்சார தரவு மாற்றம்

   ஈ. மின்சார வணிகமயமாக்க

Chapter 17.indd 285 4/11/2020 11:50:41 AM

9. தேவையற்ற மின்னஞ்சல் அடுத்தவர்களுக்கு பறிமாற்றம் செய்தல்

அ. ஊழல்
ஆ. ஸ்பேம் – மின்னஞ்சல் குப்பைகள்
இ. மோசடி
ஈ. ஸ்பூபிங் (சுருளாக்கம்)

10. பறிமாற்றத்திற்கான சட்ட அனுமதியை செயல்படுத்துவது

அ. மின்னணு தரவு உள் பறிமாற்றம்
ஆ. மின்னணு தரவு பரிமாற்றம்
இ. மின்னணு தரவு மாற்றம்
ஈ. இணைய சட்டம்

II குறுவினா (2 மதிப்பெண்கள்)

1. ஹார்வஸ்டிங் என்றால் என்ன?
2. வார்ஸ் என்றால் என்ன?
3. கிராக்கிங் சிறு குறிப்பு வரைக.
4. இரண்டு வகையான இணையதள தாக்குதல் பற்றி எழுதுக.
5. குக்கி என்றால் என்ன?

III பெருவினா (3 மதிப்பெண்)

1. பையர்வாலின் பங்கு பற்றி எழுதுக?
2. குறியாக்கம் மற்றும் மறைகுறியாக்கம் பற்றி எழுதுக.
3. மறைமுக (proxy) சேவையகம் - விவரி.
4. கணினி பயனர் பின்பற்றும் வழி காட்டுதல்கள் பற்றி எழுதுக?
5. நெறி முறை சிக்கல் என்றால் என்ன? பெயர்களை எழுதுக.

III பெருவினாக்கள் (5 மதிப்பெண்கள்)

1. கணிப்பொறி பயன்படுத்தும் போது ஏற்படும் பல்வேறு குற்றங்கள் யாவை?
2. களவாடல் என்றால் என்ன? களவாடலின் வகைகள் யாவை? மேலும் அதை எவ்வாறு தடுக்கலாம்?
3. இணையதள தாக்குதலின் வகைகளை விவரி?

துணை நூல்கள்:

- Computer Network Security and Cyber Ethics by Joseph MiggaKizza
- "Investigating Cyber Law and Cyber Ethics: Issues, Impacts and Practices: 1" by Alfreda Dudley and James Braman