សេចក្តីផ្តើម និងវត្ថុបំណងរួមនៃវគ្គសិក្សា "សន្តិសុខសាយប័រ (Cybersecurity)"

សេចក្តីផ្តើមរួម៖
សូមស្វាគមន៍មកកាន់វគ្គសិក្សា "សន្តិសុខសាយប័រ (Cybersecurity)"។ នៅក្នុងពិភពឌីជីថលបច្ចុប្បន្ន ដែលទិន្នន័យជើរតួនាទីយ៉ាងសំខាន់ និងការគម្រាមកំហែងតាមអនឡាញកាន់តែរីកចម្រើន ការយល់ដឹង និងការអនុវត្តសន្តិសុខសាយប័រជាកាតព្វកិច្ចដ៏សំខាន់សម្រាប់មនុស្សគ្រប់រូបដែលត្រូវតែស្វែងយល់។
វគ្គសិក្សានេះត្រូវបានរៀបចំឡើងដើម្បីផ្តល់ជូនលោកអ្នកនូវចំណេះដឹងទូលំទូលាយ ជំនាញជាក់ស្តែង និងឥរិយាបថប្រកបដោយការប្រុងប្រយ័ត្ន ដើម្បីការពារខ្លួនពីការគំរាមកំហែងតាមអនឡាញ។
យើងនឹងស្វែងយល់ពីរបៀបដែលមេរោគ កម្មវិធីលួចព័ត៌មាន និងការបោកប្រាស់តាមអ៊ីនធឺណិត អាចបង្កគ្រោះថ្នាក់ដល់ទិន្នន័យ និងឯកជនភាពផ្ទាល់ខ្លួន រួមទាំងវិធីសាស្ត្រការពារប្រកបដោយប្រសិទ្ធភាព ដូចជាការប្រើប្រាស់ Antivirus, Firewall, ការសម្គាល់គេហទំព័រក្លែងក្លាយ និងការគ្រប់គ្រងពាក្យសម្ងាត់ប្រកបដោយសុវត្ថិភាព។
វគ្គសិក្សានេះមានគោលបំណងផ្តល់ជូនលោកអ្នកនូវសមត្ថភាពដើម្បីក្លាយជាអ្នកប្រើប្រាស់ឌីជីថលប្រកបដោយការយល់ដឹង និងសុវត្ថិភាព។

វត្ថុបំណងរួមនៃវគ្គសិក្សា (ផ្តោតលើ ចំណេះដឹង ជំណាន និង ឥរិយាបថ):

បន្ទាប់ពីបញ្ចប់វគ្គសិក្សានេះ សិក្ខាកាមនឹងទទួលបាននូវសមត្ថភាពពេញលេញទាំងផ្នែកចំណេះដឹង ជំណាន និងឥរិយាបថដូចខាងក្រោម៖

១. ចំណេះដឹង (Knowledge)

- **ពន្យល់ពីគោលគំនិតមូលដ្ឋាន:** យល់ដឹងច្បាស់លាស់ និងអាចពន្យល់ពីនិយមន័យ គោលបំណងចម្បងនៃសន្តិសុខសាយប័រ តួនាទីរបស់ Antivirus និង Firewall។
- **កំណត់អត្តសញ្ញាណការគំរាមកំហែង:** កំណត់អត្តសញ្ញាណ និងរៀបរាប់ពីប្រភេទនៃការគំរាមកំហែងសាយប័រទូទៅបំផុត រួមមាន Malware, Virus, Worm, Trojan Horse, Ransomware, Online Scam, Phishing និងគេហទំព័រក្លែងក្លាយ។
- **យល់ដឹងពីសារៈសំខាន់នៃសុវត្ថិភាពអ៊ីនធឺណិត:** បណ្តុះចំណេះដឹងអំពីសារៈសំខាន់នៃសុវត្ថិភាពអ៊ីនធឺណិត ការប្រើប្រាស់ឌីជីថលដោយមានការយល់ដឹង។

- **យល់ដឹងពីការគ្រប់គ្រងពាក្យសម្ងាត់:** យល់ដឹងច្បាស់ពីអ្វីជាពាក្យសម្ងាត់ អត្ថប្រយោជន៍នៃកម្មវិធីគ្រប់គ្រងពាក្យសម្ងាត់ (Password Manager) និងរបៀបបង្កើតពាក្យសម្ងាត់រឹងមាំ។

២. បំណិន (**Skills**)

- **ប្រើប្រាស់ឧបករណ៍ការពារ:** ប្រើប្រាស់មុខងារមូលដ្ឋានរបស់កម្មវិធី Antivirus (ដូចជាការ Update និង Scan) និងកំណត់រចនាសម្ព័ន្ធ Firewall កម្រិត Software (ឧទាហរណ៍៖ Windows Defender Firewall) សម្រាប់អនុញ្ញាត ឬបដិសេធការភ្ជាប់កម្មវិធីជាក់លាក់។
- **សម្គាល់ និងជៀសវាងហានិភ័យ:** បង្កើនសមត្ថភាពក្នុងការសម្គាល់ហានិភ័យអនឡាញ ពិនិត្យ Link និង Website មិនសុវត្ថិភាព ការជៀសវាងសារ Phishing និងអនុវត្តជំហានសុវត្ថិភាពក្នុងការប្រើប្រាស់គណនី ឧបករណ៍ និងបណ្តាញសង្គម។
- **គ្រប់គ្រងពាក្យសម្ងាត់:** អនុវត្តការបង្កើត និងគ្រប់គ្រងពាក្យសម្ងាត់បានត្រឹមត្រូវ រក្សាទុកពាក្យសម្ងាត់យ៉ាងមានសុវត្ថិភាពដោយប្រើប្រាស់កម្មវិធីគ្រប់គ្រងពាក្យសម្ងាត់ដូចជា Google Password Manager, Apple iCloud Passwords & Keychain ឬ Lastpass។
- **អនុវត្តសុវត្ថិភាពគណនី:** អនុវត្តរបៀបធ្វើឱ្យពាក្យសម្ងាត់រឹងមាំ និងថែរក្សាគណនីបានល្អ ដោយប្រើប្រាស់គំនិតដែលអាចបង្កើតពាក្យសម្ងាត់បានល្អ។

៣. ឥរិយាបថ (**Attitude**)

- **ការប្រុងប្រយ័ត្ន:** បង្កើតទម្លាប់បម្រុងប្រយ័ត្ន និងមានទំនួលខុសត្រូវខ្ពស់ក្នុងការប្រើប្រាស់អ៊ីនធឺណិត ដោយបង្កើនការយកចិត្តទុកដាក់ មិនឆាប់ជឿលឿននូវព័ត៌មានដែលមិនច្បាស់លាស់។
- **ទំនួលខុសត្រូវឌីជីថល:** អនុវត្តឥរិយាបថសុវត្ថិភាពឌីជីថលជារឿយៗក្នុងជីវិតប្រចាំថ្ងៃ ដើម្បីការពារទិន្នន័យផ្ទាល់ខ្លួន ព័ត៌មានហិរញ្ញវត្ថុ និងឯកជនភាព។
- **ស្មារតីការពារខ្លួនឯង:** មានស្មារតីការពារខ្លួនឯង និងអ្នកនៅជុំវិញពីការគំរាមកំហែងតាមអនឡាញ។
- **ការយល់ដឹងជាបន្តបន្ទាប់:** មានឆន្ទៈក្នុងការស្វែងយល់ និងធ្វើបច្ចុប្បន្នភាពចំណេះដឹងអំពីសន្តិសុខសាយប័រជាប្រចាំ ដើម្បីទប់ទល់នឹងការគំរាមកំហែងថ្មីៗ។