

សម្រាប់មួយ។

ការវាយប្រហារតាមអ៊ីនធឺណិត

ការវាយប្រហារតាមអ៊ីនធឺណិតបានកើនឡើងក្នុងរយៈពេលដប់ឆ្នាំចុងក្រោយនេះ។ ស្វែងយល់ពីរបៀបការពារខ្លួនអ្នកពីការបាត់បង់ប្រាក់ ការលួចព័ត៌មានផ្ទាល់ខ្លួន និងការខូចខាតដល់កេរ្តិ៍ឈ្មោះ និងសុវត្ថិភាពរបស់អ្នក។



តើអ្នកដឹងទេ...

នៅឆ្នាំ 2023 មជ្ឈមណ្ឌលបណ្តឹងឧក្រិដ្ឋកម្មអ៊ីនធឺណិតរបស់ FBI បានទទួល **880,000 ពាក្យបណ្តឹង** អំពីការវាយប្រហារតាមអ៊ីនធឺណិតដែលជាលទ្ធផល **12.5 ពាន់លានដុល្លារអាមេរិក ខាតបង់**



ការវាយប្រហារតាមអ៊ីនធឺណិតគឺជាការប៉ុនប៉ងព្យាបាទក្នុងការចូលប្រើ ឬបំផ្លាញឧបករណ៍។ អ្នកវាយប្រហារតាមអ៊ីនធឺណិតអាចលួចអត្តសញ្ញាណរបស់អ្នក ប្រព្រឹត្តការក្លែងបន្លំ រារាំងការចូលប្រើឯកសាររបស់អ្នក និងវិនាសដល់រដ្ឋាភិបាល អាជីវកម្ម និងហេដ្ឋារចនាសម្ព័ន្ធសំខាន់ៗ។

ការពារខ្លួនអ្នកប្រឆាំងនឹង ការវាយប្រហារតាមអ៊ីនធឺណិត

- ចាក់សោឧបករណ៍អេឡិចត្រូនិចទាំងអស់ដោយប្រើពាក្យសម្ងាត់។
- កំណត់ការធ្វើបច្ចុប្បន្នភាពដោយស្វ័យប្រវត្តិសម្រាប់កម្មវិធី និងប្រព័ន្ធប្រតិបត្តិការ។
- ប្រើដំណោះស្រាយកំចាត់មេរោគ ប្រឆាំងមេរោគ និងជញ្ជាំងភ្លើង ដើម្បីទប់ស្កាត់ការគំរាមកំហែង។
- ប្រើពាក្យសម្ងាត់ខ្លាំង៖ តួអក្សរ 12+ អក្សរធំ និងតូច លេខ និងតួអក្សរពិសេស។
- កុំប្រើពាក្យសម្ងាត់ដូចគ្នាសម្រាប់គណនីផ្សេងគ្នា។
- ប្រើការផ្ទៀងផ្ទាត់ពីរកត្តា។
- កំណត់ភាពស្របច្បាប់មុនពេលផ្តល់ព័ត៌មានផ្ទាល់ខ្លួន។
- កុំរក្សាទុកលិខិតសម្គាល់ការចូលនៅលើឧបករណ៍ដែលមិនគួរឱ្យទុកចិត្ត។
- បម្រុងទុកឯកសារសំខាន់ៗជាទៀងទាត់នៅក្នុងពពក ឬនៅលើថាសរឹងខាងក្រៅ។
- ពិនិត្យរបាយការណ៍គណនីហិរញ្ញវត្ថុ និងរបាយការណ៍ឥណទានរបស់អ្នកឱ្យបានទៀងទាត់។



- វាយហាយសាធារណៈមិនមានសុវត្ថិភាពទេ។ កុំចូលទៅក្នុងធនាគារ ឬគេហទំព័ររសើបផ្សេងទៀត ខណៈពេលកំពុងប្រើវា។
- ផ្លាស់ប្តូរឈ្មោះលំនាំដើម និងពាក្យសម្ងាត់នៅលើ wi-fi នៅផ្ទះ។ ប្រើពាក្យសម្ងាត់ខ្លាំងតែមួយគត់ ហើយធ្វើបច្ចុប្បន្នភាពវាជាទៀងទាត់។
- កំណត់ការធ្វើបច្ចុប្បន្នភាពដោយស្វ័យប្រវត្តិនៅលើរឿតទ័ររបស់អ្នក។
- បង្កើតបណ្តាញ Wi-Fi របស់ភ្ញៀវសម្រាប់ឧបករណ៍ដូចជាឧបករណ៍ប្រើប្រាស់ រថយន្ត និងប្រដាប់ប្រដាបក្មេងលេងដើម្បីរក្សាពួកវាដាច់ដោយឡែកពីទិន្នន័យរសើប។

ក្នុងអំឡុងពេល ការវាយប្រហារតាមអ៊ីនធឺណិត

- រកមើលសកម្មភាពមិនធម្មតា៖
 - ការគិតថ្លៃកាតឥណទាន ឬការបដិសេធ
 - គណនីមិនធម្មតានៅលើរបាយការណ៍ឥណទាន
 - ការបង្ហាត់សង្គមដែលអ្នកមិនបានធ្វើ
 - មនុស្សដែលទទួលបានអ៊ីមែលដែលអ្នកមិនដែលធ្វើ
- ផ្តាច់ចេញពីអ៊ីនធឺណិត។
- ធ្វើបច្ចុប្បន្នភាពកម្មវិធីសុវត្ថិភាពរបស់អ្នក ស្តេន និងសម្ងាត់ឧបករណ៍របស់អ្នក ឬបិទថាមពល ហើយយកវាទៅអ្នកជំនាញ។
- រាយការណ៍ពីសកម្មភាពមិនធម្មតាទៅនាយកដ្ឋាន IT សម្រាប់សាលារៀន និងការងារ។
- ទាក់ទងស្ថាប័នហិរញ្ញវត្ថុ (ធនាគារ ក្រុមហ៊ុនកាតឥណទាន ការវិនិយោគ)
- ប្រាប់ទំនាក់ទំនងរបស់អ្នកឱ្យរកមើល និងលុបអ៊ីមែល ឬសារបង្ហាត់ដែលគួរឱ្យសង្ស័យចេញពីអ្នក។ ជាច្រើនដង ទំនាក់ទំនងរបស់អ្នកនឹងទទួលបានអ៊ីមែលក្លែងបន្លំធ្វើជាអ្នក។
- កំណត់ពាក្យសម្ងាត់របស់អ្នកឡើងវិញ។

បន្ទាប់ពី ការវាយប្រហារតាមអ៊ីនធឺណិត

- ប្រសិនបើមានការបាត់បង់កំពុងប្រើប្រាស់លេខសន្តិសុខសង្គមរបស់អ្នកដោយខុសច្បាប់៖
 - ដាក់របាយការណ៍ជាមួយគណៈកម្មការពាណិជ្ជកម្មសហព័ន្ធនៅ identitytheft.gov ។
 - ទូរស័ព្ទទៅសេវាចំណូលផ្ទៃក្នុង (IRS) តាមលេខ 1-800-908-4490 ប្រសិនបើអ្នកជឿថាមានការបាត់បង់កំពុងប្រើ SSN របស់អ្នក។
- ដាក់ពាក្យបណ្តឹងជាមួយ FBI Internet Crime Complaint Center (IC3) នៅ IC3.gov។
- ស្វែងយល់ពីគន្លឹះ និងឧបករណ៍បន្ថែម៖
 - StopThinkConnect.org
 - Ready.gov/cybersecurity