ԿԱՆԳՆԵՔ | ՄՏԱԾԵՔ | ՄԻԱՑԵՔ™

Կիբեռանվտագություն101

Տանը, աշխատավայրում կամ դպրոցում մեր գնալով խորացող կախվածությունը տեխլոգիաներից պահանջում է համացանցային անվտանգության առավել լայն կիրառում: Անհատները մեր պետության պաշտպանության առաջին գիծն են առցանց ռիսկերից: Այդ իսկ պատճառով կիբեռանվտանգությունը համապարտ պատասխանատվություն է ենթադրում և պահանջում է իրազեկվածություն և զգոնություն յուրաքանչյուր քաղաքացուց, համայնքից և պետությունից:

Կիբեռանվտանգությունը համակարգչային համակարգերի պաշտպանությունն է չլիազորված հարձակումներից կամ ներխուժումից:

Կանգնե՛ք, Մտածե՛ք, Միացե՛ք™ համազգային տեղեկատվական արշավի նպատակն է հանրային իրազեկման միջոցով ուղղորդել ամերիկյան հասարակությանը դեպի առավել անվտանգ Համացանցի օգտագործում՝ կիրառելով Համացանցի ապահով օգտագործման հմտությունները: Կանգնե՛ք, Մտածե՛ք, Միացե՛ք™ տեղեկատվական արշավի գլխավոր նպատակն է օգնել ամերիկացիներին հասկանալ ոչ միայն Համացանցից օգտվելու ռիսկերը, այլև անվտանգ առցանց վարքագիծ դրսևորելու կարևորությունը:

Կիբեռանվտանգությունն ընկալելու և կիրառելու նպատակով անձինք պետք է կարողանան ճանաչել առցանց ռիսկերը, սպառնալիքները և խոցելի տեղերը, ինչպես նաև դրանց ազդեցությունը համապետական և անհատական մակարդակներում:

ԿԻԲԵՌՌԻՍԿԵՐ

- **Ող.** կիբեռտարածության մեջ վնաս պատճառելու նպատակ հետապնդող անձինք, որպիսիք են հաքերները, որոնք հափշտակում են անձնական տեղեկությունները: Բարեկամ անձինք,որոնք պատահաբար վնաս են պատճառում ցանցին, համակարգին կամ Համացանցին, օրինակ՝ աշխատակիցը, որը վնասակար համակարգչային ծրագիր է ներբեռնում ընկերության ցանց:

- **Ինչ.** չարակամ անձինք օգտվում են համացանցային անանունությունից կամ խոցելիություններից՝ օգտագործելով տարբեր բարդության մեթոդներ, ինչպիսիք են համակարգիչներից ցանցերը (botnet) կամ վիրուսները: Բարեկամ անձինք ներմուծում են սպառնալիքներ այնպիսի պարզ գործողությունների միջոցով, ինչպիսիք են անհայտ հղումներ մուտք գործելը կամ USB կրիչներ օգտագործելը:

- **Երբ.** հնարավոր չէ կանխատեսել, թե երբ տեղի կունենա կիբեռմիջադեպը:

- **Որտեղ.** կիբեռտարածությունը, որը հաճախ տեղափոխվում է Համացանց, ստեղծվում էն մատչելի է համակարգչային ցանցերից, որոնք փոխանակում են տեղեկություններ և ապահովում հաղորդակցությունը: Ի տարբերություն նյութական աշխարհի՝ կիբեռտարածությունը չունի օդային, ցամաքային ծովային և տիեզերական սահմաններ:

- **Ինչու.** բարեկամ անձինքոչ միտումնավոր կերպով և հաճախ առանց գիտության վնաս են պատճառում, մինչդեռ չարակամ անձինք կարող են ունենալ շատ տարբեր դրդապատճառներ, այդ թվում՝ գաղտնի տեղեկատվության, գումարի, վարկի, արտոնության որոնում կամ վրեժի շարժառիթ:

Կան բազում առցանց ռիսկեր: Դրանցից մի քանիսն ավելի լուրջ են, քան մյուսները: Կիբեռհանցագործների մեծ մասը խտրականություն չի դնում թիրախների նշանակման հարցում. նրանց թիրախը խոցելի համակարգչային համակարգերն են՝ անկախ նրանից, թե դրանք պատկանում են պետական մարմնի, Fortune 500-ի վարկանշային սանդղակում ընդգրկված ընկերությունների, փոքր բիզնեսների, թե անհատ օգտատիրոջ:

ԿԻԲԵՌՀՈՒՇՈՒՄՆԵՐ

Որևէ քաղաքացի, համայնք կամ պետություն ապահովագրված չէ կիբեռռիսկից, սակայն կան քայլեր, որոնք ձեռնարկելու դեպքում կարող եք նվազագույնի հասցնել միջադեպի հավանականությունը.

- Ընտրեք դժվար կռահելի գաղտնաբառեր, կանոնավոր կերպով փոփոխեք դրանք և մի հաղորդեք դրանք այլ անձանց:
- Օպտիմալացրեք ձեր օպերացիոն համակարգը, զննարկիչները և այլ կարևոր ծրագրերը՝ պարբերաբար տեղադրելով դրանց արդիական տարբերակները:
- Բաց երկխոսություն վարեք ձեր ընկերների, ընտանիքի և գործընկերների հետ համացանցային անվտանգության թեմայով:
- Օգտվեք գաղտնիության կարգավորումներից և սահմանափակեք առցանց տեղադրվող մասնավոր տեղեկությունների ծավալը:
- Զգուշացեք առցանց առաջարկներից. Եթե առաջարկը չափազանց լավն է թվում իրական լինելու համար, ապա դա այդպես է, որ կա:

Դուք հնարավորություն ունեք միանալու ձեր պետության կիբեռանվտանգության իրազեկության նախաձեռնություններին: Եթե դուք, ձեր ընտանիքի անդամները կամ ձեր կազմակերպությունը հետաքրքրված եք կիբեռանվտանգության մասին ավելի շատ տեղեկություններով և Կանգնե՛ք, Մտածե՛ք, Միացե՛ք նախաձեռնությամբ, այցելեք www.dhs.gov/stopthinkconnect.

ԱՐՁԱԳԱՆՔ ԿԻԲԵՐՄԻՋԱԴԵՊԻՆ

Հրատապ գործողությունների ձեռնարկում

Անհնար է կանխատեսել կիբեռմիջադեպերի աստիճանը, բնույթը և ժամանակը: Նախազգուշացում կարող է լինել, կարող է և չլինել: Կիբեռմիջադեպերից շատերի հայտնաբերման և բացահայտման համար կարող է շատ ժամանակ պահանջվել (շաբաթներ, ամիսներ կամ տարիներ):Եթե դուք կիբեռմիջադեպի զոհ եք, հետևեք ստորև ներկայացված քայլերին՝ մեղմելու միջադեպը և վերականգնվելու դրանից:

Հրատապ գործողություններ	• Համոզվեք, որ ձեր բոլոր համակարգերի համակարգչային ծրագրերն արդիական են: • Հակավիրուսային ստուգում իրականացրեք՝ համոզվելու, որ ձեր համակարգը վարակված կամ կասկածելի չէ:
Եթե տանն եք	• Անջատեք ձեր սարքը(համակարգիչ, խաղը, և այլն)Համացանցից: Միացած չլինելով Համացանցին՝ դուք թույլ չեք տա, որպեսզի հարձակվողը կամ վիրուսը մտնի ձեր համակարգիչ և կատարի այնպիսի գործողություններ, ինչպիսիք են անձնական տվյալների տեղորոշումը, առանձին ֆայլերիձևափոխումը կամ ջնջումը կամ ձեր սարքի օգտագործումն այլոց վրա հարձակվելու նպատակով: • Եթե ունեք հակավիրուսային ծրագրերձեր համակարգչում, արդիականացրեք վիրուսների նկարագրերը և իրականացրեք ձեր ողջ համակարգի մեխանիկական
Եթե աշխատավայրում եք	• Եթե ունեք SS բաժին, անմիջապես կապվեք դրա հետ: Որքան ավելի շուտ նրանք ուսումնասիրեն և մաքրենձեր համակարգիչն, այնքան պակաս կլինի ձեր համակարգչին կամ ցանցին միացած այլ համակարգիչներին հասցրած վնասը: • Եթե գտնում եք, որ կարող եք բացահայտած լինել զգայուն տեղեկատվություն ձեր կազմակերպության վերաբերյալ, զեկուցեք այդ մասին համապատասխան անձանց կազմակերպության ներսում, այդ թվում՝ ցանցի
Եթե հասարակական վայրում եք(դպրոց, գրադարան և այլն)	• **Անմիջապես տեղյակ պահեք գրադարանավարին, ուսուցչին կամ պատասխանատու կառավարչին:** Եթե կա SS բաժին, անմիջապես կապվեք դրա հետ:

Զեկուցե՛ք միջադեպի մասին

Հրատապ գործողություններ ձեռնարկելուց հետո ծանուցեք իրավասու մարմիններին.

- Հաղորդում ներկայացրեք տեղի ոստիկանություն, որպեսզի միջադեպը պաշտոնապես գրանցվի:
- Առցանց հանցագործության կամ խարդախության մասին զեկուցեք տեղի ԱՄՆ էլեկտրոնային հանցագործությունների աշխատանքային խմբին (United States

SecretService (USSS) Electronic Crimes TaskForce) կամ Համացանցային հանցագործությունների բողոքարկման կենտրոնին (Internet Crime Complaint Center).
- Ինքնության հափշտակության և սպառողական խարդախության մասին հաղորդեք Առևտրի դաշնային հանձնաժողովին (Federal Trade Commission).

Եղե՛ք տեղեկացված և ներգրավված

Ընթացիկ կիբեռնորություններին և սպառնալիքների մասին տեղեկացված լինելու համար.

- Դարձեք Միացյալ Նահանգների արտակարգ իրավիճակների պատրաստականության թիմի (US CERT) էլեկտրոնային նամակների հասցեատեր՝ ստանալու կիբեռանվտանգությանը վերաբերող ամենաթարմ նորությունները: Մշակված լինելով անհատական և գործարար օգտատերերի համար՝ այդ նորությունները ժամանակին տեղեկություններ են ապահովում անվտանգության ընթացիկ հարցերի և խոցելի տեղերի վերաբերյալ: Բաժանորդագրվելու համար այցելեք (Sign uphere).
- Դարձեք Հայրենիքի անվտանգության դեպարտամենտի Կանգնեք, Մտածեք, Միացեք տեղեկատվական արշավի բարեկամը և ստացեք ամսեկան նորությունների ամփոփաթերթը կիբեռանվտանգության ընթացիկ միջոցառումնեևով և հուշումներով:
- Բաժանորդագրվելու համար այցելեք (Sign up here).