

Dėl pandemijos mokymuisi persikėlus į skaitmeninę erdvę, kibernetinių atakų prieš vaikus skaičius išaugo 144 proc., teigia kibernetinio saugumo kompanija „Surfshark“. Skaičiuojama, kad dar pandemijos pradžioje nusikaltėlių aukomis kasdien tapdavo vidutiniškai 8 vaikai, o finansinių nuostolių dydis per metus siekė 610 tūkst. eurų. Didžiausiu vaikų atsparumu internetinėms grėsmėms pasidžiaugti galėjo į vaikų edukaciją aktyviai investuojančios šalys – Indija, Malaizija ir Japonija. Todėl saugumo ekspertas Aleksandr Valentij dalijasi 4 patarimais tėvams, kaip apie internetines grėsmes kalbėti su savo vaikais.

„Technologijoms tobulėjant pagrindiniu nusikaltėlių įrankiu išlieka socialinės inžinerijos technikos. Tai pasitikėjimu, melu ar akių dūmimu grįstos apgaulės, į kurias įvilioti vaikai nieko nenutuokdami patys atiduoda nusikaltėliams reikalingus duomenis. Toks apgaulės tipas vadinamas „phishingu“ ir yra populiariausias kibernetinis nusikaltimas pasaulyje visose amžiaus grupėse. Bet būtent todėl, kad yra paremtas ne aukštosiomis technologijomis, o žmogaus psichologija, nesunkiai gali būti įveiktas pasitelkus sąmoningumą ir edukaciją“, – sako Aleksandras Valentij, „Surfshark“ kibernetinio saugumo vadovas.

1. Supažindinkite vaikus su grėsmėmis

Pirmiausia, rekomenduojama vaikus supažindinti su internete egzistuojančiomis kibernetinėmis grėsmėmis ir jų tipais bei paskatinti elgtis atidžiai. Gali padėti analogija, jog kaip ir realiame gyvenime ar filmuose yra nusikaltėlių, taip jie egzistuoja ir internete.

„Jaunesnėms atžaloms galima parodyti ir specialiai jiems sukurtus kibernetinio saugumo animacinius filmukus, kuriuos nesunku rasti internete. Jie vaizdžiai, įdomiai ir vaikams suprantamai supažindina su tuo, kaip atrodo pavojai internete. Trumpą [edukacinį pasirinkimų žaidimą](#) sukūrėme ir mes – jis leidžia vaikams patiems pabandyti rasti teisingus sprendimus pavojingose situacijose“, – sako A. Valentij.

Ekspertas prideda, kad svarbu ne tik abstrakčiai, o konkrečiais pavyzdžiais paaiškinti, kaip nusikaltėliai veikia. Išsamų dažniausių ir žinomiausių nusikaltimų sąrašą ir jų aprašymus galima rasti [kibernetinio saugumo enciklopedijoje](#).

„Pradžioje vaikams pakaks pristatyti žinomiausius nusikaltimų tipus – „phishingą“ ar pasitikėjimo apgaulės, kurios ir atneša daugiausiai žalos. O vyresniems vaikams gali būti įdomu sužinoti ir daugiau pavojų, ypač kai internete jie jau naršo gerokai aktyviau ir plačiau.

Naudinga vaikams paaiškinti ir galimą žalą – tas padės jiems suprasti, kodėl šiai temai skiriate tiek dėmesio ir skatinate vaikus būti atsakingais“, – pasakoja A. Valentij.

2. Susitarkite taisykles

Išsiaiškinus galimas grėsmes, svarbu nepalikti vaikų pačių tvarkytis su jomis taip, kaip išmano. Būtina suteikti įrankius, kuriuos esant reikalui šie galėtų pasitelkti. Padės labai aiškos taisyklės, ką internete galima daryti ir ko visais įmanomais būdais vengti.

„Griežta raudona linija turėtų tapti bet koks asmeninės informacijos atskleidimas – adreso, telefono numerio, el. pašto adreso, slaptažodžių siuntimas ir bet kokios pinigų perlaidos. Taip pat svarbu priminti, kad vaikai atidžiai galvotų, kam siunčia savo, kad ir juokais padarytas, nuotraukas. Mat kartais internete nusikaltėliai apsimeta vaikų bendraamžiais ir taip siekia išvilioti informaciją“, – aiškina A. Valentij.

Taisyklės gali reikšti ir susitarimus dėl tėvų naudojamų saugumo priemonių – laiko kontrolės ar pasirinktų puslapių blokavimo įrankius.

„Rekomenduojama kompiuterio ugniasienės (angl. firewall) nustatymuose užblokuoti nepageidaujamus puslapius, namų kompiuteryje ir mobiliuosiuose telefonuose įdiegti interneto naudojimo laiko ribotuvą. Taip pat prasminga kompiuterį laikyti atviroje kambario vietoje, kad matytumėte, ką vaikas veikia. Visa tai leis, esant reikalui, užkirsti kelią pavojų keliančiam veiklai“, – sako A. Valentij.

Įvairių sričių ekspertai primena, kad vaikai turi suprasti, jog nustatytos ribos yra ne kontrolės ir bausmės mechanizmai, bet saugumo priemonės. Svarbu jas aptarti, dėl jų susitarti ir vėliau nenaudoti vaikų auklėjimui už blogą elgesį.

3. Skatinkite atvirą bendravimą

„Surfshark“ ekspertas primena, kad kalbantis su vaikais labai svarbu jų negąsdinti. Greičiau – šviesti, supažindinti ir stengtis padėti. Tokiu būdu jie ne tik greičiau pasisavins informaciją, bet ir nesigėdys, nesibaimins ir nebandys slėptis, jei koks nors incidentas vis tik nutiktų.

„Net ir tokiems reikšmingiems duomenims kaip el. paštas ir jo slaptažodis nutekėjus, įmanoma suvaldyti situaciją, jei reaguojama laiku, pavyzdžiui, slaptažodį pakeičiant ir įjungiant dviejų veiksmų autentifikacijos funkciją (angl. two-factor authentication, 2FA). O nukentėjus finansiškai privalu kreiptis į teisėsaugą. Bet tam, jog visa tai padarytumėte, vaikai apie incidentus turi jums papasakoti kiek įmanoma anksčiau. Tikėtina, jog tai jie

padarys tik žinodami, jog nebus nubausti už klaidas, todėl labai svarbu leisti jiems suprasti, kad visada gali būti ramūs kalbėdami su jumis apie netikėtumus internete“, – aiškina A. Valentij.

Ekspertas prideda, kad atvirumas svarbus ne tik incidentų atvejais, bet ir tiesiog naršant internete ir naudojant kompiuterį. Su vaikais būtina susitarti, kad tėvams paprašius parodyti, ką vaikas veikia namų kompiuteryje, jaunuoliai bet kada turi tą padaryti.

„Labai svarbu, kad tai netaptų perdėtos kontrolės ar vaiko privatumo pažeidimais, bet tėvai turi atidžiai stebėti, ką vaikai veikia internete. Savo praktikoje turėjau ne vieną atvejį, kai nusikaltėliams apsimetus vaikų bendraamžiais, šie būdavo atakuojami net ir tėvams esant šalia. Tad svarbu aktyviai domėtis ir klausti, ką vaikai veikia. Antraip, nekreipiant dėmesio į ekraną, sukuriamas tik apgaulingas saugumo jausmas“, – aiškina A. Valentij.

4. Kartu apsaugokite paskyras

Apsisaugoti nuo kibernetinių nusikaltėlių atakų padeda ne tik sąmoningumas ir edukacija, bet ir įprasti saugumo įrankiai.

„Svarbus tvirtas paskyrų ir įrenginių slaptažodis, dviejų veiksmų autentifikacijos funkcija, geros antivirusinės programos ar ugniasienės. Viešose vietose vaikams žaidžiant telefonu ar naršant internete prasminga naudoti ne viešą bevielį „Wi-Fi“ tinklą, bet mobiliuosius duomenis, arba apsaugoti ryšį virtualiu privačiu tinklu (angl. virtual private network, VPN)“, – teigia A. Valentij.

Visų svarbiausia, kad visos šios priemonės būtų įdiegtos, bet ekspertas papildomai rekomenduoja jas paruošti kartu su vaikais.

„Matydami žingsnius, kurių imatės saugumui užtikrinti, vaikai galės mokytis juos atlikti savaime, bet daug svarbiau, kad stebėdami pavyzdį matys, kaip svarbu saugumu rūpintis atsakingai. Rimtas požiūris į saugumą ir privatumą internete yra viena svarbiausių savybių, padedanti apsisaugoti nuo socialinės inžinerijos atakų“, – sako A. Valentij.

