OUCH! | 2015 m. birželio mėn.

Mėnesinis informacinio saugumo naujienlaiškis kompiuterių naudotojams

OUCH!

ŠIAME LEIDINYJE…

- Faktai
- Pavojai
- Vaikų mokymas

Vaikų mokymas apie internetinį saugumą

Faktai

Šiandien yra nepaprastai daug būdų, kuriais vaikai gali prisijungti prie interneto ir bendrauti tarpusavy. Naujos socialinės žiniasklaidos paslaugos auga tarsi piktžolės, o internetinių programų ir žaidimų kuriama vis daugiau. Be to, daugumoje mokyklų duomenys perkeliami į tokias vietas kaip Google Drive ir reikalaujama, kad dalis ar visi jų darbai būtų atliekami ir pateikiami internetu. Taigi teoriškai vaikai yra auginami „siejant juos su internetu“. Nors tai turi daug privalumų, tačiau naudojantis šiomis galimybėmis taip pat susiduriama su pavojais. Šiame naujienlaiškyje patyrinėsime tris vaikams pavojingas sritis ir apžvelgsime būdus, kuriais galėtumėte juos apsaugoti.

Kviestinis redaktorius

Bob Rudis yra „Verizon“duomenų saugumo specialistas, 2015 m. parašęs tyrimo ataskaitą apie duomenų saugumo pažeidimus ir auginantis keturis nuostabius vaikus. Daugumoje „Fortune 100“ įmonių Bob sukūrė ir vadovavo įdomioms ir veiksmingoms programoms, kurių metu buvo skatinamas supratimas apie saugumą. Bob žinutes galite skaityti Twitter paskyroje adresu **@hrbrmstr**.

Pavojai

1. **Elgesys**: bendraudami internetinėse bendruomenėse ar virtualiuose pasauliuose, vaikai gali elgtis taip, kaip niekada nesielgtų tikrame gyvenime. Fizinio dalyvavimo stoka žmonėms, o ypač vaikams, gali sukurti galingą anonimiškumo jausmą. Todėl jie dažnai yra linkę save išreikšti tokiais būdais, kurie gali skaudinti kitus vaikus, pavyzdžiui, internetu ieškodami priekabių arba žaidimuose žudydami nepriešiškus žaidėjus. Be to, jūsų vaikai gali tapti kitų asmenų aukomis, kurie tyčia bandys juos įskaudinti ar įžeisti.

2. **Bendravimas**: dabar vaikai beveik nuolatos bendrauja su kitais, neatsižvelgiant ar tai atliekama tekstinėmis žinutėmis, bendraujant internetinėse bendruomenėse ar žaidžiant virtualiuose pasauliuose. Fiziškai nedalyvaudami jie dažnai užmiršta, jog kitame ekrano gale esantis asmuo nebūtinai yra tas, kuo sakosi esantis arba turintis teigiamų ketinimų. Šiose skaitmeninėse gatvėse klaidžiojantys grobuonys išnaudos kiekvieną strategiją, padėsiančią susidraugauti su potencialiomis aukomis, patys apsimesdami vaikais.

3. **Turinys**: internete netrūksta būdų, kuriais galima įrašyti ir paskelbti vaizdo ar garso įrašą, paveikslėlį ar tekstinę žinutę. Vaikams kyla pagunda paskelbti arba pasidalinti pernelyg dideliu kiekiu informacijos apie save arba kitus savo

Vaikų mokymas apie internetinį saugumą

šeimos narius net nesuvokiant, jog viso to padariniai yra labai rimti. Vaikai taip pat gali nesuvokti asmens tapatybės vagystės arba kenkimo programų keliamų pavojų, kai kiti jų klausia asmeninių klausimų arba prašo jų atlikti kokius nors veiksmus, pavyzdžiui, paspausti tam tikras nuorodas. Galiausiai, gyvename amžiuje, kuriame negalime atšaukti internete jau paskelbtų arba kitiems pabendrintų dalykų. Vaikai gali galvoti, kad Kik, Instagram, Snapchat ir kitose programose skelbiami įrašai yra greitai pakeičiami kitais, tačiau vėliau šie įrašai gali būti panaudoti prieš juos pačius ar jų šeimos narius.

visa vaikų mokymo apie saugų buvimą interneto tinkle esmė yra ta, kad ne tik jūs, bet ir vaikai apie tai kalba su jumis.

Vaikų mokymas

Pirmas dalykas, kurį galite padaryti, norėdami apsaugoti vaikus, tai su jais pasikalbėti. Sužinokite, ką jūsų vaikai veikia internete, pamokykite juos apie šiuolaikinius pavojus ir kaip jie turėtų elgtis, norėdami apsisaugoti.

1. **Saugumas namuose**: viskam greitai besikeičiant, namai turėtų tapti ta vieta, kurioje būtų mokoma saugaus internetinio elgesio. Kuo anksčiau pradėsite tarpusavy kalbėtis, tuo bus geriau. Nuolatos kalbėkitės apie internetinio saugumo problemas, parodydami tikrus jau įvykusius neigiamus pavyzdžius. Jei nežinote, ką veikia jūsų vaikai, tiesiog paklauskite jų. Suvaidinkite neišmanančius tėvus ir paprašykite vaikų jums parodyti, kokios šiuo metu yra naujausios technologijos ir kaip jie jomis naudojasi. Vaikams patinka būti mokytojais, todėl jie atsivers. Pavyzdžiui, jei jie naudoja Instagram, paprašykite jų jums parodyti, kaip Instagram veikia ir sukurti jums paskyrą, kuria naudodamiesi, stebėkite juos. Taip ne tik žinosite ir stebėsite, ką jūsų vaikai veikia, bet ir padarysite, kad jiems būtų lengviau su jumis šnekėtis. Be to, pasistenkite – tiek, kiek galite – padaryti taip, kad visa internetinė veikla būtų vykdoma centrinėje namų vietoje ir nustatykite, kiek laiko jie gali naudotis internetu. Kompiuterius pastačius centrinėje namų vietoje, vaikai bus kur kas mažiau linkę elgtis pavojingai. Taip pat pamąstykite apie centrinę mobiliųjų įrenginių krovimo vietą, sukurdami taisyklę, kad visi mobilieji įrenginiai turi būti palikti toje vietoje, kai vaikai vakare eis miegoti.

2. **Saugumas svečiuojantis pas kitus**: vaikams būnant ne namie, jie gali susidurti su didesne rizika. Paaiškinkite jiems, kad jūsų internetinės taisyklės galioja visur, kur tik jie yra ir papasakokite apie šiuos apribojimus tiems, kurie juos prižiūri. Jei jie turi mobiliuosius įrenginius, patikrinkite naudojimosi įpročius (laiką ir trukmę), norėdami

Vaikų mokymas apie internetinį saugumą

pamatyti ar yra požymių, rodančių, jog būdami ne namie jie mažiau paiso apribojimų. Jūs negalėsite sustabdyti visų pažeidimų, tačiau norėdami žvilgtelėti į savo mobiliuosius įrenginius, jie prisimins jūsų rūpestingus žodžius.

3. **Saugumas skaičiais**: jūs nesate vieninteliai, kurie yra stebimi internete, todėl norėdami padėti savo tėvams, globėjams, broliams, seserims, mokytojams ir draugams išvengti galimai grėsmingo elgesio, turėtumėte juos įtraukti į šią veiklą. Paskatinkite bendruomenę stebėti vaikus ir gražiai su jais apie tai pasikalbėti, pamačius, jog vaikai pradėjo elgtis pavojingai.

Galiausiai, vaikams suklydus, tokius įvykius laikykite patirtimi, iš kurios jie gali pasimokyti, o ne nedelsdami imkitės drausminių priemonių. Kaskart paaiškinkite „kodėl“ jie turėtų elgtis vienaip ar kitaip ir priminkite, kad jūs tik stengiatės juos apsaugoti nuo pavojų, kurių jie dar nemato. Informuokite juos, kad jie visada gali į jus kreiptis, jei bendraudami internetu susidurtų su kažkuo nemaloniu, o galbūt net pamokykite, jog jie turėtų jums persiųsti ekrano vaizdo kopiją. Įsitikinkite, jog jiems nėra nepatogu į jus kreiptis, susivokus, jog padarė kažką nederamo. Galimybės suteikimas aktyviai bendrauti realiame gyvenime tai geriausias būdas apsaugoti vaikus šiuolaikiniame skaitmeniniame pasaulyje.

SUŽINOKITE DAUGIAU

Prenumeruokite kas mėnesinį OUCH! naujienlaiškį, gaukite prieigą prie archyvų, sužinokite daugiau apie SANS saugumo sprendimus apsilankę http://www.securingthehuman.org.

Šaltiniai

Cyber Smart: http://www.cybersmart.gov.au/Parents.aspx

OnGuard Online: http://www.onguardonline.gov/topics/protect-kids-online

Būk saugus tinkle: https://www.staysafeonline.org/stay-safe-online/for-parents/raising-digital-citizens

Apie vaikų saugumą:
http://www.rsaconference.com/media/into-the-woods-protecting-our-youth-from-the-wolves-of-cyberspace

Licencija

Redaktoriai: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis

Lietuvišką vertimą finansavo „Perlo“ įmonių grupė.