WEB OF SCIENTIST: INTERNATIONAL SCIENTIFIC RESEARCH JOURNAL
ISSN: 2776-0979, Volume 3, Issue 3, Mar., 2022

ISSUES OF EDUCATION OF AWARENESS FEELINGS AGAINST INFORMATION ATTACK, CYBER ATTACK

Khudoikulov Golibjon Tolibovich
Teacher of Kashkadarya Academic Lyceum of the Ministry of Internal Affairs,
Master of the Pedagogical Institute of Karshi State University

Annotation
As cyberattackers continue to exploit vulnerabilities and introduce new threats and vulnerabilities, teachers, parents and students should also be equipped with the knowledge to protect their devices and personal information. Thanks to the many advances in modern technology, online learning is more convenient than ever, allowing students to experience the high-quality experiences and outcomes that traditional education provides through a virtual experience.

Keywords: cyber activity, information attack, cyber attackers, youth.

Аннотация
Поскольку кибератаки продолжают использовать уязвимости и внедрять новые угрозы и уязвимости, учителя, родители и учащиеся также должны быть оснащены знаниями для защиты своих устройств и личной информации. Благодаря многочисленным достижениям в области современных технологий онлайн-обучение стало более удобным, чем когда-либо, позволяя учащимся испытать высококачественный опыт и результаты, которые традиционное образование обеспечивает посредством виртуального опыта.

Ключевые слова: кибератиность,информационная атака, киберзлоумышленники, молодежь.

Annotatsiya
Kiberhujumchilar bo'shliqlardan foydalanishda va yangi tahdidlar va zaifliklarni kiritishda davom etar ekan, o'qituvchilar, ota-onalar va o'quvchilar ham o'z qurilmalari va shaxsiy ma'lumotlarini himoya qilish bo'yicha bilimlar bilan jihozlanishi kerak. Zamonaviy texnologiyalarning ko'plab yutuqlari tufayli onlayn ta'lim har qachongidan ham qulayroq bo'lib, o'quvchilarga virtual tajriba orqali an'anaviy ta'lim taqdim etadigan yuqori sifatli tajriba va natijalarni olish imkonini beradi.

WEB OF SCIENTIST: INTERNATIONAL SCIENTIFIC RESEARCH JOURNAL
ISSN: 2776-0979, Volume 3, Issue 3, Mar., 2022

Kalit so`zlar: kiberfaoliyat, axborot xuruji, kiberhujumchilar, yoshlar.

Kirish

Yoshlar uchun kiberxavfsizlik

Zararli kiberfaoliyat yoshlarga turli yo'llar bilan ta'sir qiladi, odatda zararli dasturlar va firibgarlik ko'rinishida bo`ladi. Education Technology ma'lumotlariga ko'ra, bu yil yoshlar shaxsiy kompyuterlari va uy Wi-Fi tarmoqlaridan foydalangan holda darslarga qo'shilishlari sababli, potentsial hujum vektorlari soni tez ko'paydi. Hujumning oldini olishdan oldin, bu bugungi yoshlar duch keladigan tahdidlar haqida kuchli tushunchaga ega bo'lishdan boshlashga yordam beradi. Bu erda xabardor bo'lish kerak bo'lgan besh turdagi hujumlar:

- Ma'lumotlarni o'g'irlash: CNBC ma'lumotlariga ko'ra, kiberhujumchilar o'quvchilar odatda birinchi marta onlayn kiritilgan shaxsiy va moliyaviy ma'lumotlarni qanday qilib to'g'ri himoya qilishni tushunishmaydi. Mutaxassislarning ta'kidlashicha, xakerlar bu ma'lumotlardan shaxsiy ma'lumotlarni o'g'irlash, kredit firibgarligi va boshqalar uchun foydalanishi mumkin.
- Mobil zararli dastur: Check Point tadqiqotchilari 2018-yildan beri mobil qurilmalarga qaratilgan hujumlar 50 foizga oshganini aniqladilar. Koʻproq yoshlar ish stoli yoki noutbukdan smartfon foydalanishga oʻtayotgani sababli, mobil xavfsizlikka jiddiy yondashish har qachongidan ham muhimroq.
- Ijtimoiy tarmoqdagi zararli xabarlar: COVID-19 pandemiyasi davrida kiberxavfsizlik tahdidlari boʻyicha oʻtkazilgan tadqiqotga koʻra, xakerlar shaxsiy maʼlumotlarini buzishi mumkin boʻlgan fishing veb-saytlariga qurbonlarni jalb qilish uchun Facebook va WhatsApp kabi platformalardan firibgarlik yoʻli bilan foydalanmoqda.
- Kamera bilan ishlash: Bugungi kunda ko'plab yoshlar o'zlarining telefonlari, planshetlari yoki noutbuklarida ish stoli veb-kameralari yoki kameralariga ega. Afsuski, bu xakerlar veb-kameraga masofadan kirish va nazorat qilish imkoniyatiga ega bo'lgan kamerani suratga olish uchun eshikni ochishi mumkin.
- Ijtimoiy muhandislik: EducationDive ma'lumotlariga ko'ra, ijtimoiy muhandislik firibgarliklari oliy ta'lim yoshlari duch keladigan kiberxavfsizlik tahdidlaridan biridir. Ushbu hujumlar maxfiy ma'lumotlarni oshkor qilish uchun foydalanuvchilarni manipulyatsiya qilishga tayanadi. Yoshlar uchun kiberxavfsizlik bo'yicha maslahatlar.

WEB OF SCIENTIST: INTERNATIONAL SCIENTIFIC RESEARCH JOURNAL
ISSN: 2776-0979, Volume 3, Issue 3, Mar., 2022

Adabiyotlar Tahlili Va Metodologiyasi

Bugungi kiber xakerlar doimiy ravishda foydalanuvchilarni buzish uchun yangi ekspluatatsiyalar va strategiyalarni kashf qilmoqdalar. Yoshlarni ulardan himoya qilishga yordam beradigan beshta eng yaxshi kiberxavfsizlik amaliyoti:

- Shaxsiy ma'lumotlarni almashishdan saqlaning: Internetda oshkor qiladigan ma'lumotlarga, masalan, maktab nomlari, elektron pochta manzillari, uy manzillari va telefon raqamlari haqida ehtiyot bo'ling.
- Viruslardan himoya qilishga investitsiya qiling: Barcha qurilmalarda (ish stoli kompyuterlari, noutbuklar, planshetlar va boshqalar) o'rnatilgan anti-fishing yordami bilan antivirus himoyasi mavjudligiga ishonch hosil qiling. Uni avtomatik ravishda yangilanadigan qilib sozlang va kamida haftasiga bir marta viruslarni skanerlang.
- Dasturiy ta'minotni yangilab turing: operatsion tizimingiz, brauzer dasturlari va ilovalarni yamoqlar bilan to'liq yangilangan holda saqlang. Hatto yangi mashinalarda ham sizni xavf ostiga qo'yishi mumkin bo'lgan eskirgan dasturiy ta'minot bo'lishi mumkin.
- Fishingdan ehtiyot bo'ling: ishonchsiz manbalardan kelgan elektron pochta qo'shimchalarini ochmang. Guruh aʼzolari yoki oʻqituvchilaridan elektron pochta xabarlarini kutayotgan boʻlishingiz mumkin, ammo qoʻshimchalarni ochishda ehtiyot boʻling.
- Bosganingizda ehtiyot bo'ling: noma'lum veb-saytlarga tashrif buyurishdan yoki ishonchsiz manbalardan dasturiy ta'minotni yuklab olishdan saqlaning. Ushbu saytlar kompyuteringizni o'rnatadigan (ko'pincha jimgina) zararli dasturlarni joylashtirishi mumkin.

Kiberxavfsizlik faqat auditoriyada - virtual yoki boshqa tarzda cheklanmasligi kerak. Aksariyat uy tarmoqlari institutlar tomonidan taqdim etilgan xavfsizlik devori yoki himoya vositalarini ta'minlamaganligi sababli, o'qituvchilar va yoshlar internetda ko'proq vaqt o'tkazishlari sababli xakerlik urinishlariga ko'proq moyil bo'lishadi. Hamma joyda xavfsiz onlayn xulq-atvorni qo'llash muhimdir. O'qituvchilar uchun kiber tahdidlar

O'qituvchi sifatida xabardor bo'lish va yoshlarni va yoshlaringizni himoya qilishning eng yaxshi amaliyotlarini o'rganish har doim kiberxavfsizlikda qo'yiladigan eng yaxshi birinchi qadamdir.

Fishing: Ushbu hujumlar qurbonlarni parollar yoki kredit karta ma'lumotlari kabi nozik ma'lumotlardan voz kechish uchun aldash uchun inson hissiyotlaridan foydalanish orqali ijtimoiy muhandislikdan foydalanadi. Ma'lumotlarga ko'ra, bugungi kunda kiberhujumlarning 90% dan ortig'i fishing bilan boshlanadi.

Taqsimlangan xizmatni rad etish (DDoS): Ushbu hujumlar bir nechta tizimlar mahalliy serverlarning tarmoqli kengligi yoki resurslarini to'ldirganda sodir bo'ladi. Ushbu hujumlar qurbonlarga soatiga 40 000 dollarga tushishi mumkin, odatda kiberhujumchilar uchun muhandislik qilish uchun atigi 40 dollar turadi.

Ma'lumotlarning buzilishi: Ma'lumotlarning buzilishi shaxsiy yoki maxfiy ma'lumotlarga (yoshlar ma'lumotlari kabi) ruxsatsiz kirish mumkin bo'lgan xavfsizlik hodisasidir. Aslida, yoshlar va o'qituvchilar ma'lumotlarining buzilishi 2019 yilda eng ko'p uchraydigan kiber hodisalardan biri bo'ldi.

Ransomware: Bu tahdidlar pul yoki boshqa talablar evaziga ma'lumotlarni garovga olgan xakerlarni o'z ichiga oladi. Emisof kiberxavfsizlik firmasi hisobotiga ko'ra, 2019 yilda Qo'shma Shtatlardagi to'lov dasturining potentsial qiymati 7,5 milliard dollardan oshdi.

IoT zaifliklari: Noutbuklar, aqlli uy aksessuarlari va planshetlar kabi IoT (Internet of Things) qurilmalari ko'pincha xavfsizlikka ega emas yoki muntazam ravishda yangilanmaydi, bu o'qituvchilar uchun IoT qurilmalarini sinfga kiritishda xavfsizlikni birinchi o'ringa qo'yishini juda muhim qiladi.

Kompyuter ta'limi assotsiatsiyasi tomonidan taqdim etilgan ushbu hujumlarning oldini olishga yordam beradigan beshta qadam:

Ma'lumotlarni shifrlash: Bugungi kunda xakerlar sinf ma'lumotlarini tranzit paytida ushlab qolish orqali olishlari mumkin. Shifrlash yordamida ma'lumotlarni himoya qilish orqali kiberhujumchilar yuborilgan va qabul qilgan ma'lumotlarni o'g'irlashining oldini olish mumkin.

Tashkilotingizning kiberprotokollariga rioya qiling: Sizning maktabingizda foydalanuvchilarni himoya qilish uchun allaqachon kiberxavfsizlik choralari mavjud. Agar muammo yuzaga kelsa, ushbu qoidalarga rioya qilish va AT yoki kiberxavfsizlik bo'limi bilan bog'lanish muhim.

Qurilmalaringizni jismoniy hujumlardan himoya qiling: uzoqlashganda har doim kompyuteringizdan chiqing. Parollarni xavfsiz saqlash uchun ularni yozib qo'ymang yoki hisob ma'lumotlaringizni boshqa birovning nazarida kiritmang.

Ma’lumotlaringizni zaxiralang: Agar ishingiz yoki muassasangiz yoshlar ma’lumotlarini saqlashni talab qilsa, tajovuzkorlar ushbu shaxsiy ma’lumotlarni Ransomware uslubidagi hujumlarda nishonga olishiga yo‘l qo‘ymaslik uchun ularning zaxira nusxasini yaratish muhim, bunda to‘lov to‘lanmaguncha blokirovka qilinadi.

Parolni yaxshi boshqarishni mashq qiling: Parollar haqida gap ketganda, yorliqlarni ishlatish oson. LastPass kabi parollarni boshqarish dasturi barcha hisoblaringiz uchun noyob parollarni saqlashga yordam beradi.

Masofaviy ta'limda yoshlar ma'lumotlarini himoya qilishda muhim ahamiyatga ega 3 ta kiberxavfsizlik bo'yicha maslahatlar

- To'xtating. O'ylang. Ulanish. Ota-onalar va o'qituvchilar resurslari
- Ma'lumotlaringizni qanday zaxiralash mumkin
- Parol menejeridan qanday foydalanish
- Uyda kiberxavfsizlik: Ota-onalar nimani bilishi kerak

Shaxsan o'rganish haqida gap ketganda, maktablar odatda o'quvchilarga zararli kontentga kirishni cheklaydigan ishonchli himoyani taklif qiladi, shu bilan birga ularni zararli dasturlar yoki boshqarilmaydigan ijtimoiy media kabi keng qamrovli tahdidlardan himoya qiladi. Bunga odatda maktab qurilmalariga qo'llaniladigan filtrlar va qora ro'yxatlar (foydalanuvchilar kirish imkoni bo'lmagan veb-saytlar to'plami) yoki maktabning tarmoq ulanishi orqali erishiladi. Biroq, yosh o'quvchilar raqamli sinflarga murojaat qilganda, ota-onalar rasmiy muassasalar tomonidan o'rnatilgan bir xil himoya vositalaridan foydalana olmasligi mumkin.

Ota-Onalar Va Bolalar Uchun Kiber Tahdidlar

PCMag hisobotiga ko'ra, ota-onalarning 76 foizi o'z farzandlarining onlayn xavfsizligidan xavotirda va bolalar duch keladigan onlayn tahdidlardan katta xavotirda.

Quyida yosh veb-foydalanuvchilarga qaratilgan beshta keng tarqalgan kiberhujumlarni sanab o'tdik.

Kiber yirtqichlar: Bular internetdan bolalar va/yoki o‘smirlarga zarar yetkazish maqsadida (hissiy, moliyaviy va h.k.) foydalanish uchun foydalanadigan kattalardir. Bolalarning onlayn ekspluatatsiyasi haqida xabar berish uchun Kanadadagi Cybertip kompaniyasi COVID-19 pandemiyasi boshlangandan beri hisobotlarda 81% ga oshganini xabar qildi.

Zararli dasturiy ta'minot: Bugungi kunda kiber jinoyatchilar ko'pincha qurbonlarni aldab, o'zlarining qurilmalarini boshqarishi mumkin bo'lgan zararli dasturlarni yuklab olishadi. Ba'zi kiber jinoyatchilar hatto o'zlarining zararli dasturlarini o'yin yoki ilovalar sifatida yashirishi mumkin, bu ayniqsa bolalarni vasvasaga solishi mumkin.

Zararli reklamalar: Bu reklamalar turli xil kiruvchi xabarlar yoki spamlarni tarqatish uchun ishlatiladi. Michigan universiteti va CS Mott bolalar kasalxonasi tadqiqotchilari yaqinda yosh bolalar uchun mo'ljallangan 135 ta ilovani tahlil qilishdi va ularning ko'plarida muammoli reklama usullari, jumladan, manipulyatsiya va uyatchanlik bilan to'lib-toshganligini aniqladilar.

Shaxsni o'g'irlash: Bugungi kiber hujumchilar bolalarning shaxsiy ma'lumotlari va kredit tarixini o'g'irlash uchun onlayn tarzda nishonga olishmoqda. Darhaqiqat, Javelin Strategy & Research Study 2017-yilda bir milliondan ortiq bolalar firibgarlik qurboni bo‘lganini va buning natijasida jami 2,6 milliard dollar zarar ko‘rgan va oilalarga 540 million dollardan ortiq mablag‘ yo‘qolgan.
Onlayn o'yinlar: Ko'ngilochar dasturiy ta'minot assotsiatsiyasining tadqiqotiga ko'ra, oilalarning 70 foizida kamida bitta bola video o'yin o'ynaydi. Webroot ma'lumotlariga ko'ra, ko'plab bolalar faol o'yin o'ynashi bilan firibgarlik, viruslar va ta'qiblar o'yin jamoalarida odatiy holga aylangan.

Mulohaza takliflar

Ota-onalar va bolalar uchun kiberxavfsizlik bo'yicha maslahatlar

Ota-ona sifatida siz farzandingiz uchun yuqorida aytib o'tilganlar kabi onlayn tahdidlardan eng yaxshi himoyasisiz. Farzandingiz bilan bugun bajarishni boshlashingiz mumkin bo'lgan beshta qadam:

- Parollar va maxfiylikni o'rgating: Farzandlaringizga barcha qurilmalar va onlayn hisoblarni parol bilan himoyalashga yordam bering. Ularga kuchli parollar yaratish nima uchun muhimligini, ularni qanday yaratishni va ularni hech qachon baham ko'rmaslikni o'rgating.
- Kuzatish va muloqot qilish: Qabul qilinadigan, hurmatga sazovor (o'zlari va boshqalar uchun) onlayn postni o'z ichiga olgan narsalarni bildiring va farzandingizning onlayn faoliyatini imkon qadar tez-tez kuzatib borish uchun vaqt ajrating.
- Shaxs va joylashuvni himoyalash: Android yoki iPhone-da suratga geotag qo‘yishni o‘chirib qo‘ying va bolangizga yoshi, maktabi, manzili, telefon raqami, familiyasi yoki shaxsini aniqlash mumkin bo‘lgan har qanday shaxsiy ma’lumotlarni internetda baham ko‘rmaslikni eslatib qo‘ying.
- Xavfsiz Wi-Fi-dan foydalaning: Uyingizdagi Wi-Fi tarmog'ida shifrlash va tashqi kirishni cheklash uchun kuchli parol mavjudligiga ishonch hosil qiling va parolingizni faqat yoshlarni bilgan va ishonadiganlar bilan baham ko'ring.
- Ota-ona nazorati vositalaridan foydalaning: Ko'pgina bolalar qo'llaridagi quvvatni to'liq tushuna olishlaridan oldin ularga birinchi planshet yoki internetga ulangan qurilma beriladi. Ehtiyot choralarini ko‘rish va ulardan foydalanishni imkon qadar tezroq kuzatish uchun o‘rnatilgan ota-ona nazorati funksiyalaridan foydalanib ko‘ring.

Ota-Onalar Uchun Qo'shimcha Manbalar

- Kuchli parollarni yaratish va boshqarish
- Yoshlarni himoya qilish uchun kiberxavfsizlik bo'yicha tezkor havolalar
- Ota-onalar uchun shaxsiy hayotga intiluvchan bolalarni tarbiyalash bo'yicha maslahatlar
- Smartfonda ota-ona nazoratidan qanday foydalanish
- Uy Wi-Fi tarmog'ida ota-ona nazorati qanday o'rnatiladi

Xulosa

Kiberhujumchilar bo'shliqlardan foydalanishda va yangi tahdidlar va zaifliklarni kiritishda davom etar ekan, o'qituvchilar, ota-onalar va o'quvchilar ham o'z qurilmalari va shaxsiy ma'lumotlarini himoya qilish bo'yicha bilimlar bilan jihozlanishi kerak.

Zamonaviy texnologiyalarning ko'plab yutuqlari tufayli onlayn ta'lim har qachongidan ham qulayroq bo'lib, o'quvchilarga virtual tajriba orqali an'anaviy ta'lim taqdim etadigan yuqori sifatli tajriba va natijalarni olish imkonini beradi. Biroq, bu yutuqlar bilan kiber jinoyatchilar tomonidan kengaytirilgan tahdid paydo bo'ladi. Yoshlarni xavfsiz saqlash har qachongidan ham muhimroq. Yuqoridagi maslahatlarga amal qilish texnologiya va shaxsiy ma’lumotlaringizni kiberjinoyat tahdidlaridan yaxshiroq himoya qilishga yordam beradi. Axborot tizimlari va infratuzilmasining kiberxavfsizligi so‘nggi yillarda eng muhim masalalardan biriga aylandi. Ko'p odamlar, ham bolalar, ham kattalar, Internet orqali ulangan kompyuter tarmoqlariga kirish uchun kundalik hayotida mobil telefonlar va planshetlar kabi portativ qurilmalardan foydalanadilar. Biroq, internetdan foydalanish umumiy ilovalardan foydalanadigan ko'plab vositalardan foydalanishni o'z ichiga olganligi sababli, navigatsiya, ma'lumotlarga kirish, ijtimoiy tarmoqlardagi tendentsiyalar, yangiliklar kontenti, ko'ngilochar va ofis ilovalari (elektron pochta, kalendar va boshqalar) ham mavjud. Foydalanuvchi identifikatorini o'g'irlash, shaxsiy daxlsizlikni buzish, zararli kodlar, kiberbullying va boshqalar kabi xavf-xatarlar uchun maydonga aylanish mumkin. Adabiyotda kiberxavfsizlik o'rganilgan bo'lsa-da, kam sonli tadqiqotlar kiberxavfsizlikdan xabardorlik va foydalanuvchilarning kiberxavfsizlik xulq-atvoriga befarqligi bilan bog'liq. Bundan tashqari, turli xil foydalanuvchilar klasterlarining kiberxavfsizlik tahdidlaridan xabardorligi (masalan, IT-mutaxassislari va nomutaxassislar, yoshi kattaroq va yosh foydalanuvchilar) to‘liq baholanmagan. Ushbu maqolaning maqsadi - boshlang'ich va o'rta maktab o'quvchilari kabi foydalanuvchilarning turli klasterlarining kiberxavfsizlikdan xabardorligi bilan bog'liq nazariy va amaliy echimlarni taqdim etish orqali jismoniy shaxslarning kiber

xabardorligini oshirish va shu bilan ularni xavfsizroq va yaxshiroq ish va hayot uchun jihozlash va tayyorlashdir. Shu sababli, ushbu maqolaning maqsadlari quyidagilardan iborat: 1. Baholangan ta'lim tizimlari va amaliyotining har bir darajasida o'quv dasturlarini o'zgartirish bo'yicha tavsiyalar ishlab chiqish. 2. Ta’limning barcha darajalarida o‘quv dasturlarini o‘zgartirish bo‘yicha tavsiya etilgan tavsiyalardan foydalangan holda kiber xabardorlik bo‘yicha ta’lim tizimini (CAEF) ishlab chiqish. Biz kiber xabardorlik bo'shlig'iga qaysi omillar ta'sir ko'rsatishini va aniq tavsiyalar orqali bo'shliqni qanday qisqartirish yoki hatto yo'q qilishni, ya'ni ta'lim tizimining turli darajalarida o'quv dasturlarida shaxslarning kiber xabardorligini qanday yaxshilashni tushunishni kutamiz.

Adabiyotlar Ro`Yxati

1. Iqtisodiy va informatsion xavfsizlik zamonaviy muammolari»mavzuidagi yosh olimlarning respublika ilmiy-amaliy konferentsiyasi materialari to`plami (20 dekabr’ 2005 yil). Nashr uchun ma`sulM.M. Baxadirov.T.. JIDU,2006.
2. Yarochkin.V.I. Informatsionnaya bezopasnost’. Uchebnik dlya studentov VUZov.M.. Akademicheskiy proekt Fond «Mir»,2003.-
3. Informatsiya.Diplomatiya.Psixologiya.M.: «Izvestiya»,2002.
4. V.I. Xozikov.Informatsionnoe orujie. Sankt-Peturburg.Izdatel’skiy Dom «Neva», Moskva.Izdatel’stvo «OLMA-PRESS Obrazovanie»,2003.
5. Lopatin V.N. Informatsionnaya bezopastnost’ Rossii: CHelovek. Obshestvo. Gosudarstvo Sankt-Peturburg. Izd. MVD Rossii i Sankt-Peturburgskogo universiteta (Fond «Universitet»).2000.
6. Natsionnal’naya bezopastnost’: Informatsionnaya. Sostavlyayushaya V.V. Eremenko, Yu.I. Kovalenko i dr.; pod red.V.V. Eremenko. -M.: MOSU,2000.-