ULOVI LIKA S WEBA KOJI TVOJE € VREBA

WEB HEROJ_

Financira
Europska unija
NextGenerationEU

RH MUP

POLICIJA
RH MUP

Ulovimo lika s weba koji tvoje € vreba

PROJEKT „JAČANJE KAPACITETA POLICIJE ZA SUZBIJANJE KIBERNETIČKOG KRIMINALITETA"

Neočekivano ste osvojili nevjerojatnu ponudu za putovanje?! Potvrdili ste je klikom „Slažem se", ali, nažalost, ni traga ni glasa ni putovanja ni novca. Odlučili ste uložiti u kriptovalute koje su obećavale goleme profite, no, nažalost, vaš je novac nestao bez traga. Očekivali ste dolazak voljenog doktora iz egzotične zemlje i platili mu putovanje?! Nažalost, oženio vas je, ali samo za novac! Sve su ovo samo neki od primjera kibernetičkih prijevara koje prevaranti koriste kako bi vam ukrali novac. Kako biste ih preduhitrili, ključno je znati prepoznati znakove i biti na oprezu.

OVAJ MALI VODIČ OTKRIT ĆE VAM SVE O VRSTAMA PRIJEVARA, KAKO IH PREPOZNATI TE SE USPJEŠNO ZAŠTITITI I UNAPRIJEDITI SVOJU RAČUNALNU SIGURNOST.

Internet je postao neizostavan dio našeg svakodnevnog života, a sve više građana i poslovnih subjekata prepoznaje njegovu važnost kao platformu za poslovanje i komunikaciju. Zbog toga je postao iznimno privlačan kibernetičkim kriminalcima koji koriste iznimno sofisticirane trikove i obećanja kako bi dobili novac ili vrijedne financijske informacije od svojih žrtava. Posljedice takvih prijevara su ozbiljne, dovode do financijskih gubitaka, gubitka povjerenja, narušavanja ugleda i često izazivaju dugotrajni emocionalni stres kod žrtava i njihovih obitelji. Kako bismo smanjili vjerojatnost da postanemo žrtva, najučinkovitiji način je ponašanje koje se temelji na samozaštiti, a to postižemo informiranošću i educiranjem.

Projekt „Jačanje kapaciteta policije za suzbijanje kibernetičkog kriminaliteta" koji provodi Ministarstvo unutarnjih poslova u sklopu Nacionalnog plana oporavka i otpornosti namijenjen je jačanju kapaciteta policije nabavom računalnih sustava za istraživanje otvorenih izvora na internetu i Darknetu te za specijalizirane treninge policijskih službenika za kibernetički kriminalitet.

U sklopu projekta provodi se i preventivna kampanja „Web heroj" čiji je cilj osvijestiti i educirati građane o nužnosti i načinima zaštite u virtualom svijetu kako ne bi postali žrtve tih kaznenih djela.

AKO NEŠTO NIJE ISTINITO U STVARNOM SVIJETU, NIJE NI U VIRTUALNOM. AKO PRIMIJETITE BILO ŠTO SUMNJIVO, SVAKAKO TO PRIJAVITE POLICIJI.

PRIJEVARA S RAČUNIMA

KOJI JE NAČIN IZVRŠENJA?

Prevarant pristupa tvrtki te se pretvara da je dobavljač, davatelj usluga, vjerovnik.
Može se koristiti kombinacija pristupa putem telefona, pisma, e-pošte itd.
Prevarant traži da se bankovni podaci o plaćanju, odnosno pojedinosti o bankovnom računu primatelja budućih računa promijene. Novi navedeni račun kontrolira prevarant.

ŠTO MOŽETE PODUZETI?

KAO PODUZEĆE/KOMPANIJA/TVRTKA

Osigurajte da su zaposlenici obaviješteni i svjesni ovih oblika prijevare te upućeni kako ih izbjeći.
Upozorite osoblje odgovorno za plaćanje računa da ih uvijek provjeravaju zbog mogućih nepravilnosti.
Uvedite postupak provjere autentičnosti zahtjeva za plaćanjem.
Pregledajte informacije objavljene na mrežnoj stranici tvrtke, posebno ugovore i dobavljače.
Osigurajte da vaši zaposlenici budu oprezni s dijeljenjem informacija o tvrtki na svojim društvenim mrežama.

KAO DJELATNIK/ZAPOSLENIK

Redovito provjeravajte sve zahtjeve koji izgledaju kao da dolaze od vaših vjerovnika, posebno ako traže promjenu bankovnih podataka za buduća plaćanja.
Za isplate iznad određenog praga, uspostavite postupak koji zahtijeva potvrdu ispravnosti bankovnog računa i primatelja (npr. organizirajte sastanak s tvrtkom).
Nemojte koristiti kontakte dobivene putem pisama, faxa, e-pošte koji traže izmjene. Sigurnije je koristiti one iz prethodne korespondencije.
Odredite osobe koje će biti jedinstvene kontaktne točke za komunikaciju s tvrtkama kojima redovito plaćate.
Ograničite dijeljenje informacija o svom poslodavcu na društvenim mrežama.
Nakon što ste platili račun pošaljite e-poruku primatelju kako biste ga obavijestili o plaćanju.
Kao mjeru sigurnosti, navedite naziv banke i posljednje četiri znamenke računa na koji ste izvršili uplatu.

U SLUČAJU POKUŠAJA PRIJEVARE, UVIJEK SE OBRATITE POLICIJI, ČAK I AKO NISTE POSTALI ŽRTVA.

DIREKTORSKA PRIJEVARA

„Direktorska" prijevara je oblik prijevare u kojoj zaposlenik koji ima ovlasti za obavljanje plaćanja bude prevaren da plati lažni račun ili izvrši neovlašteni prijenos s računa tvrtke.

Prevarant obično zove ili šalje poruke predstavljajući se kao direktor ili član uprave tvrtke.

Prevarant je dobro upoznat s organizacijom tvrtke.

Traži hitnost u izvršavanju plaćanja i koristi fraze poput „povjerljivost", „tvrtka ima povjerenje u vas" ili „trenutačno sam nedostupan".

Često se zahtjevi odnose na međunarodna plaćanja prema bankama izvan Europe.

Zaposlenik prenosi sredstva na račun koji kontrolira prevarant.

Upute o tome kako postupiti mogu biti dane kasnije, putem treće osobe ili e-pošte.

Zaposlenika se traži da zaobiđe redovne postupke autorizacije.

Često tvrde da je riječ o osjetljivoj situaciji poput porezne kontrole ili preuzimanja i spajanja poduzeća.

KOJI SU ZNAKOVI?

- Iznenadan poziv/poruka.
- Nametanje pritiska i naglašavanje hitnosti.
- Izravni kontakt od visokog dužnosnika u tvrtki s kojim obično niste u kontaktu.
- Nesvakidašnji zahtjev koji se protivi internim postupcima.
- Traži se potpuna povjerljivost.
- Prijetnje, neuobičajene pohvale ili obećanja nagrade.

ŠTO VI MOŽETE NAPRAVITI?

KAO PODUZEĆE/KOMPANIJA/TVRTKA

Budite svjesni rizika i osigurajte da vaši zaposlenici budu informirani i upoznati s rizicima.
Potaknite zaposlenike da budu oprezni pri svim zahtjevima za plaćanje.
Redovito provodite interne procedure vezane uz plaćanja.
Uvedite postupak provjere autentičnosti zahtjeva za plaćanje putem e-pošte.
Usvojite pravila za prijavu prijevara.
Redovito pregledavajte informacije objavljene na internetskim stranicama vaše tvrtke, ograničite dijeljenje informacija i budite oprezni s društvenim mrežama.
Nadogradite i redovito ažurirajte tehničke sigurnosne mjere.

UVIJEK SE OBRATITE POLICIJI U SLUČAJU POKUŠAJA PRIJEVARE, ČAK I AKO NISTE POSTALI ŽRTVA.

KAO DJELATNIK/ZAPOSLENIK

Strogo se pridržavajte sigurnosnih protokola za plaćanja i nabavu. Ne preskačite nijedan korak i nemojte popustiti pritisku. Uvijek pažljivo provjeravajte adrese e-pošte kada je riječ o osjetljivim informacijama ili prijenosu sredstava. Ako imate sumnje u vezi zahtjeva za prijenos, obratite se nadležnom kolegi. Nikad ne otvarajte sumnjive poveznice ili privitke primljene putem e-pošte. Budite posebno oprezni kada čitate svoju privatnu e-poštu na računalima tvrtke. Ograničite dijeljenje informacija i budite oprezni s društvenim mrežama. Izbjegavajte dijeljenje informacija o organizaciji tvrtke, sigurnosti i postupcima.

AKO PRIMITE SUMNJIVU E-POŠTU ILI POZIV,
ODMAH OBAVIJESTITE ODJEL ZA IT.

INVESTICIJSKA PRIJEVARA

Najčešće prijevare u vezi s investicijama uključuju ponude za unosna ulaganja poput dionica, obveznica, kriptovaluta, plemenitih metala, stranih zemljišta ili alternativne energije.

KAKO PREPOZNATI UPOZORAVAJUĆE ZNAKOVE?

Primate učestale iznenadne pozive.
Obećavaju vam brzu i golemu dobit te vas uvjeravaju u sigurnost investicije.
Ponuda je dostupna samo na ograničeno vrijeme.
Uvjeravaju vas kako je ponuda dostupna samo vama i traže da je ne dijelite s drugima.

ŠTO MOŽETE PODUZETI?

Uvijek zatražite nepristrani financijski savjet prije nego što uložite novac.
Odbijte iznenadne pozive o mogućnostima ulaganja.
Budite sumnjičavi prema ponudama koje obećavaju veliku dobit, zajamčen povrat ili sigurna ulaganja.
Ako ste već bili žrtva prijevare, prevaranti će vjerojatno pokušati ciljati na vas ponovno ili prodati vaše podatke drugim prevarantima, stoga budite na oprezu.
Ako primijetite nešto sumnjivo, obratite se policiji.

PRIJEVARA PRI ONLINE KUPNJI

Posebna ponuda - kupi! SUPER POPUST 70%

Iako su online ponude često primamljive, važno je biti oprezan kako biste izbjegli prijevare.

KAKO SE ZAŠTITITI?

Koristite lokalne online trgovine kad god je to moguće – vjerojatnije je da ćete lakše riješiti moguće probleme. Uložite malo truda i istražite te provjerite recenzije prije nego što obavite kupnju.
Koristite svoje kartice za plaćanje – imat ćete veće šanse za povrat novca u slučaju prijevare.
Plaćajte samo putem sigurnih pružatelja usluga plaćanja – budite oprezni ako traže prijenos sredstava preko banke ili alternativnih načina plaćanja. Razmislite dvaput prije nego što pristanete!
Plaćajte samo kada ste povezani na sigurnu internetsku vezu – izbjegavajte korištenje besplatnih ili otvorenih javnih Wi-Fi mreža.
Plaćajte samo na sigurnom uređaju – redovito ažurirajte operativni sustav i sigurnosni softver. Pazite se oglasa koji nude nevjerojatne ponude ili čudotvorne proizvode – ako zvuče predobro da bi bili istiniti, vjerojatno i nisu!
Ako vam iskoči oglas koji tvrdi da ste osvojili nagradu, budite oprezni – mogla bi biti riječ o zlonamjernom softveru. Ako naručeni proizvod ne stigne, kontaktirajte prodavača. Ako ne dobijete odgovor, obratite se svojoj banci.

Uvijek prijavite svaku sumnju na pokušaj prijevare policiji, čak i ako niste postali žrtva.
Pametno kupujte i zaštitite se od online prijevara!

ROMANTIČNA PRIJEVARA

Prevaranti ciljaju potencijalne žrtve na online stranicama za upoznavanje, ali također i društvene mreže i e-poštu kako bi uspostavili kontakt.

KAKO PREPOZNATI UPOZORAVAJUĆE ZNAKOVE?

Osoba koju ste nedavno upoznali online iskazuje snažne osjećaje prema vama i želi da uspostavite privatne razgovore.

Poruke koje primate od njih često su loše napisane i nejasne.

Njihov online profil ne odražava ono što vam govore.

Mogu vas tražiti da im pošaljete intimne fotografije ili videozapise o sebi.

Prvo pokušavaju zadobiti vaše povjerenje. Zatim traže novac, darove ili traže podatke o vašem bankovnom računu ili kreditnoj kartici.

Ako odbijete poslati novac, mogu vas pokušati ucjenjivati. Ako im ipak pošaljete novac, tražit će još više.

ŠTO MOŽETE PODUZETI?

Budite iznimno oprezni pri dijeljenju osobnih podataka na društvenim mrežama i stranicama za upoznavanje.

Uvijek budite svjesni rizika čak i na renomiranim platformama i stranicama.

Idite polako i postavljajte pitanja kako biste upoznali osobu.

Provjerite fotografiju i profil osobe kako biste vidjeli jesu li već korišteni na drugim mjestima.

Pazite na pravopisne i gramatičke pogreške te nedosljednosti u njihovim pričama. Također, budite sumnjičavi ako imaju izgovore da njihova kamera ne radi.

Ne dijelite nikakav kompromitirajući materijal koji bi mogao biti iskorišten za ucjenu.

Ako se dogovorite za osobni susret, obavijestite svoju obitelj i prijatelje o lokaciji na koje idete.

Budite oprezni sa zahtjevima za novcem. Nikada ne šaljite novac, podatke o kartici, online računu ili kopije osobnih dokumenata.

Izbjegavajte bilo kakva plaćanja unaprijed.

ŠTO AKO STE POSTALI ŽRTVA?

Nemojte se osjećati krivima ili nelagodno!

Odmah prekinite svaki kontakt s prevarantom.

Ako je moguće, sačuvajte svu komunikaciju, uključujući chat poruke.

Prijavite slučaj policiji.

Prijavite internetsku stranicu na kojoj je prevarant prvi put stupio u kontakt s vama.

Ako ste podijelili podatke o svom računu, odmah se obratite banci.

„PHISHING" MREŽNA KRAĐA IDENTITETA

Krađa identiteta je oblik prijevare koji uključuje slanje lažnih e-poruka kojima se obmanjuje primatelja i navodi ga se na dijeljenje osobnih, financijskih ili sigurnosnih podataka.

KOJI JE NAČIN IZVRŠENJA?

Takve e-poruke mogu biti iznimno slične legitimnoj korespondenciji koju banke zaista šalju.

One vjerno reproduciraju logotipove, izgled i ton pravih e-poruka.

Često traže da preuzmete priloženi dokument ili kliknete na poveznicu.

Koriste izraze koji stvaraju dojam hitnosti.

Počinitelji računalnih kaznenih djela često iskorištavaju činjenicu da su ljudi zauzeti; na prvi pogled, takva lažna e-poruka može izgledati legitimno.

ŠTO MOŽETE PODUZETI?

Redovito održavajte svoj softver uključujući preglednik, antivirusni program i operativni sustav.

Budite posebno oprezni kada dobijete e-poruku koja izgleda kao da dolazi od vaše „banke" i traži osjetljive podatke poput lozinke za vaš online račun.

Pažljivo pregledajte e-poštu: usporedite e-adresu s prethodnim stvarnim porukama koje ste dobili od svoje banke. Provjerite pravopis i gramatiku.

Nemojte odgovarati na sumnjivu e-poruku, već je proslijedite svojoj banci tako da sami upišete njenu adresu.

Ne klikajte na poveznice i ne preuzimajte privitke, već ručno upišite adresu u svoj preglednik.

Ako niste sigurni, provjerite na službenoj stranici banke ili nazovite njezinu službu za korisnike.

Budite oprezni prilikom korištenja mobilnog uređaja. Na pametnom telefonu ili tabletu može biti teže primijetiti pokušaje krađe identiteta.

KRAĐA IDENTITETA SMS-om

Poznat kao kombinacija riječi SMS i Phishing (krađa identiteta), Smishing je oblik prijevare koju prevaranti koriste kako bi dobili pristup vašim osobnim, financijskim ili sigurnosnim podacima putem tekstualnih poruka.

KOJI JE NAČIN IZVRŠENJA?

U SMS poruci često se traži da kliknete poveznicu ili nazovete telefonski broj radi „potvrde", „ažuriranja" ili „ponovne aktivacije" vašeg računa, međutim, ta veza vodi do lažne internetske stranice, a telefonski broj pripada prevarantu koji se pretvara da je legitimna tvrtka.

ŠTO MOŽETE PODUZETI?

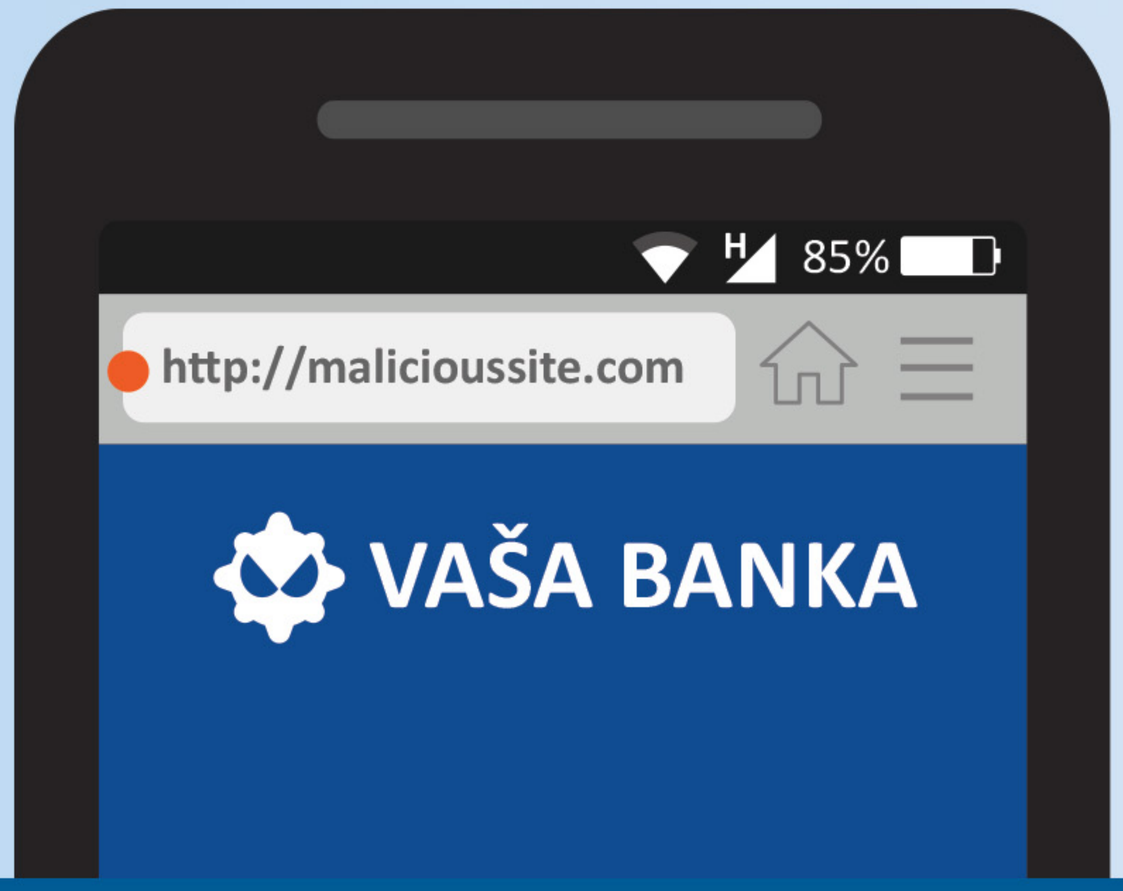
Prije nego što kliknete na poveznice, privitke ili fotografije koje ste primili u SMS porukama s nepoznatog broja, obavezno provjerite identitet pošiljatelja.

Nemojte se požurivati. Uzmite si vrijeme za odgovarajuće provjere prije nego što odgovorite na poruku.

Nikada ne odgovarajte na SMS poruke koje traže vaš PIN, lozinku za online bankarstvo ili bilo koje druge sigurnosne vjerodajnice.

Ako sumnjate da ste postali žrtva smishinga i ako ste već podijelili bankovne podatke, odmah se obratite svojoj banci.

LAŽNE STRANICE BANAKA



Često se događa da e-pošta, koja se čini kao da dolazi od banke, sadrži poveznice koje vode do lažnih mrežniih stranica banaka. Na tim stranicama prevaranti će vas zatražiti da otkrijete svoje financijske i osobne podatke. Budite oprezni i ne nasjedajte na takve prijevare.

KAKO PREPOZNATI UPOZORAVAJUĆE ZNAKOVE?

Lažne stranice banaka vrlo vjerno imitiraju izgled pravih bankovnih stranica. Na tim lažnim stranicama često će se pojaviti prozor koji traži unos bankovnih vjerodajnica. Važno je znati da stvarne banke ne koriste takve prozore za prikupljanje osjetljivih informacija. Budite oprezni i izbjegavajte dijeljenje svojih bankovnih podataka na sumnjivim stranicama.

ZNAKOVI PREPOZNAVANJA NA LAŽNIM STRANICAMA

Hitnost: takve poruke naglašavaju hitnost i pritisak da odmah poduzmete određene radnje. Važno je napomenuti da prave stranice banaka ne upotrebljavaju takve metode za komunikaciju s korisnicima.

Loš dizajn: budite oprezni s internetskim stranicama koje imaju neobičan dizajn ili sadrže pravopisne i gramatičke pogreške. To su znakovi da stranica može biti lažna.

Skočni prozori: ove stranice često koriste skočne prozore koji traže unos osjetljivih informacija poput korisničkih imena, lozinki ili financijskih podataka. Nemojte kliknuti na te prozore niti unositi svoje osobne podatke na takve sumnjive stranice.

Budite oprezni i provjerite autentičnost stranica banke prije nego što dijelite bilo kakve osjetljive informacije ili poduzmete radnju na takvim sumnjivim stranicama.

ŠTO MOŽETE PODUZETI?

Nikada nemojte klikati na poveznice u porukama koje tvrde da vode do vaše banke. Umjesto toga, preporučuje se da ručno upišete adresu mrežne stranice banke u preglednik ili koristite postojeću vezu koju ste već dodali u svoj popis „favorita" ili „bookmarka".

Kada pregledavate sadržaj interneta s mobilnog uređaja, budite pažljivi i osigurajte da je vaša veza sigurna putem HTTPS protokola. Uvijek provjerite nalazi li se na početku URL adrese. I ne zaboravite, zbog manje veličine zaslona mobilnih uređaja, URL adrese prikazuju se u ograničenom prostoru, što može otežati provjeru.

Također je preporučljivo koristiti preglednik koji omogućuje blokiranje skočnih prozora. To će vam pomoći u sprječavanju otvaranja neželjenih prozora koji mogu sadržavati lažne stranice ili tražiti vaše osjetljive podatke.

Važno je napomenuti da ako postoji nešto važno ili hitno što banka mora podijeliti s vama, obavijestit će vas putem sigurnog kanala kada pristupite svom online računu. Stoga, nema potrebe da odgovarate na sumnjive poruke ili poveznice izvan sigurnog okruženja vašeg bankovnog računa.

KRAĐA IDENTITETA POZIVOM

Vishing (kombinacija riječi Voice i Phishing) je oblik telefonske prijevare u kojoj prevaranti koriste glasovne pozive kako bi navodili žrtvu da otkrije svoje osobne, financijske ili sigurnosne podatke ili da izvrši uplatu novčanih sredstava.

ŠTO MOŽETE PODUZETI?

Budite oprezni kada primite neočekivani telefonski poziv.

Zabilježite broj pozivatelja i recite im da ćete ih nazvati povratno.

Kako biste potvrdili njihov identitet, pronađite službeni telefonski broj organizacije i kontaktirajte ih izravno.

Ne provjeravajte autentičnost pozivatelja koristeći broj koji su vam oni dali jer bi mogao biti lažan ili krivotvoren.

Prevaranti mogu prikupiti osnovne informacije o vama putem interneta (npr. društvene mreže). Nemojte pretpostavljati da je pozivatelj legitimna osoba samo zato što ima te podatke.

Nikada ne dijelite PIN kartice ili lozinku za online bankarstvo. Vaša banka nikada neće tražiti te informacije.

Ne šaljite novac na račun na zahtjev nepoznate osobe. Vaša banka nikada neće tražiti takvu transakciju.

Ako sumnjate da je poziv lažan, prijavite ga svojoj banci.

SAMO IGRA?

Instalirajte aplikacije samo sa službenih trgovina aplikacijama.

APPS

Prije preuzimanja aplikacije, istražite i aplikaciju i njezine izdavače. Pazite na internetske poveznice koje dobivate u e-pošti i SMS porukama koje vas mogu prevariti da instalirate aplikacije treće strane ili iz nepoznatih izvora.

PROVJERITE RECENZIJE I OCJENE DRUGIH KORISNIKA

PROČITAJTE DOPUŠTENJA APLIKACIJE

Provjerite kojim vrstama podataka aplikacija može pristupati te dijeli li vaše informacije s vanjskim stranama. Jesu li aplikaciji potrebna sva ta dopuštenja? Ako nisu, nemojte je preuzeti.

INSTALIRAJTE APLIKACIJU ZA MOBILNU SIGURNOST

Ona će pregledati sve aplikacije na vašem uređaju i svaku novu koju naknadno instalirate te vas obavijestiti ako pronađe zlonamjerni softver.

ZLONAMJERNI SOFTVER MOŽE VAS KOŠTATI

ZLONAMJERNI SOFTVER ZA MOBILNO BANKARSTVO

Zlonamjerni softver za mobilno bankarstvo napravljen je za krađu financijskih informacija pohranjenih na vašem uređaju.

KAKO SE ŠIRI?

- Posjećivanjem zlonamjernih internetskih-mjesta
- Preuzimanjem zlonamjernih aplikacija
- Krađom identiteta

KOJI SU RIZICI?

- Snimanje osobnih informacija za potvrdu autentičnosti
- Neovlašteno podizanje gotovine

ŠTO MOŽETE UČINITI?

- Preuzmite službenu mobilnu aplikaciju svoje banke i pazite da svaki put posjećujete stvarnu internetsku-lokaciju banke. **https://**
- Nemojte dopustiti da vas internetska-stranica ili aplikacija za bankarstvo automatski prijavljuju.
- Ni s kim nemojte dijeliti ili otkrivati broj bankovne kartice ili lozinku.
- Ako je dostupna, instalirajte aplikaciju za mobilnu sigurnost koja će vas upozoriti na svaku sumnjivu aktivnost.
- Ako izgubite mobilni telefon ili promijenite broj, obratite se banci kako bi oni mogli ažurirati vaše informacije.
- Informacije o svom računu nemojte dijeliti putem tekstualne poruke ili e-pošte.
- Kada se povezujete s bankovnom internetskom-stranicom ili aplikacijom, uvijek koristite sigurnu Wi-Fi mrežu.
- Često provjeravate svoje financijske izvatke.

POZDRAVITE SE S OSOBNIM DATOTEKAMA

MOBILNI SOFTVER KOJI TRAŽI OTKUPNINU

Softver koji traži otkup drži vaš uređaj i podatke kao taoce i postavlja cijenu. Ova vrsta zlonamjernog softvera zaključava zaslon vašeg uređaja i sprječava pristup nekim datotekama i značajkama.

KAKO SE ŠIRI?

- Posjetom ugroženim internetskim-mjestima.
- Preuzimanjem lažnih verzija legitimnih aplikacija.
- Klikom na zlonamjerne internetske-poveznice i privitke ugrađene u poruke e-pošte koje kradu identitet.

KOJI SU RIZICI?

- Morate uređaj vratiti na tvorničke postavke i tako izgubiti sve podatke.
- Napadač može dobiti potpun pristup vašem uređaju i podijeliti vaše podatke s trećim stranama.

ŠTO MOŽETE UČINITI?

- Često stvarajte sigurnosne kopije podataka te ažurirajte aplikacije i operativni sustav.
- Izbjegavajte kupnju u trgovinama aplikacija treće strane.
- Ako je dostupna, instalirajte aplikaciju za mobilnu sigurnost koja će vas upozoriti ako vam je uređaj ugrožen.
- Čuvajte se poruka e-pošte i internetska- mjesta koja izgledaju umnjivo ili djeluju predobro da bi bila istina.
- Nikome nemojte davati administrativne ovlasti.
- Nemojte plaćati otkupninu. Financirat ćete kriminalce i ohrabriti ih da nastave s protuzakonitim aktivnostima.

ZLONAMJERNI SOFTVER MOŽE VAS KOŠTATI

KORISNI SAVJETI ZA TVRTKE

1 OBAVIJESTITE ZAPOSLENIKE O MOBILNIM RIZICIMA

Mobilni rad zamućuje granicu između poslovne i osobne upotrebe. Tvrtke mogu pretrpjeti golemu štetu napadom koji je inicijalno bio usmjeren na mobilni uređaj pojedinca. Mobilni uređaj je računalo i potrebno ga je zaštititi kao što štitite računala.

2 UVEDITE KORPORATIVNU POLITIKU 'DONESI SVOJ UREĐAJ' (BRING-YOUR-OWN-DEVICE, BYOD)

Zaposlenici koji koriste svoje mobilne uređaje da bi pristupali korporativnim podacima i sustavima (čak i ako je riječ samo o bazama podataka e-pošte, kalendaru ili kontaktima), moraju slijediti pravila tvrtke. Pažljivo odaberite tehnologije koje ćete koristiti za upravljanje mobilnim uređajima i njihovo osiguravanje te uputite zaposlenike da budu oprezni.

3 UKLJUČITE PRAVILA MOBILNE SIGURNOSTI U UKUPNI SIGURNOSNI OKVIR

Ako uređaj nije sukladan sa sigurnosnim pravilima, ne bi mu se smjelo dopustiti spajanje s korporativnom mrežom te pristup korporativnim podacima. Tvrtke bi trebale implementirati rješenja za upravljanje mobilnim uređajima (MDM) ili upravljanje mobilnošću tvrtke (EMM). Uz to sve, ključno je instalirati rješenje za obranu od mobilnih prijetnji. To će osigurati povećanu vidljivost i kontekstualnu svijest o aplikacijama, mreži te prijetnjama na razini operacijskog sustava.

4 BUDITE OPREZNI PRI KORIŠTENJU JAVNIH WI-FI MREŽA KOD PRISTUPA PODACIMA TVRTKE

Općenito govoreći, javne Wi-Fi mreže nisu sigurne. Ako zaposlenik pristupa korporativnim podacima koristeći javnu Wi-Fi mrežu u zračnoj luci ili u kafiću, podaci mogu biti izloženi zlonamjernim korisnicima. Savjetuje se da tvrtke razviju pravila „učinkovitog korištenja“ kad je o tome riječ.

5 NEKA OPERACIJSKI SUSTAVI I APLIKACIJE UREĐAJA BUDU AŽURIRANI

Savjetujte osoblju da preuzme ažuriranja softvera za operacijske sustave uređaja čim ih se to zatraži. Posebno za Android, istražite davatelje mobilnih usluga i proizvođače uređaja da biste doznali njihovu politiku ažuriranja. Najnovija ažuriranja zajamčit će veću sigurnost uređaja, ali i njegove bolje performanse.

6 INSTALIRAJTE APLIKACIJE SAMO S PROVJERENIH IZVORA

Kod mobilnih uređaja koji se povezuju s korporativnom mrežom, tvrtke bi trebale dopustiti instalaciju samo aplikacija sa službenih izvora. Možete i razmisliti o izradi korporativne trgovine aplikacijama putem koje krajnji korisnici mogu pristupati aplikacijama koje je odobrila tvrtka, preuzimati ih i instalirati. Obratite se davatelju usluga sigurnosti i zatražite savjet ili izradite svoj sustav sigurnosti unutar tvrtke.

7 SPRIJEČITE „OTVARANJE“ UREĐAJA (JAILBREAK POSTUPAK)

„Otvaranje“ je postupak uklanjanja sigurnosnih ograničenja koja nameće davatelj operacijskog sustava kako bi se dobio potpun pristup operacijskom sustavu i značajkama. Otvaranje uređaja može znatno oslabiti njegovu sigurnost i otvoriti sigurnosne rupe koje možda nisu bile vidljive. Upotreba uređaja kojima je otvoren sustav ne bi smjela biti dopuštena u okruženju tvrtke.

8 RAZMISLITE O ALTERNATIVAMA POHRANE U OBLAKU

Mobilni korisnici često žele pristupiti važnim dokumentima, ne samo putem službenih računala nego i putem privatnih mobitela ili tableta izvan ureda. Tvrtke bi trebale pristupiti izradi sigurne pohrane u oblaku te uslugama sinkronizacije datoteka kako bi riješile te potrebe na siguran način.

9 POTAKNITE OSOBLJE DA INSTALIRA APLIKACIJU ZA MOBILNU SIGURNOST

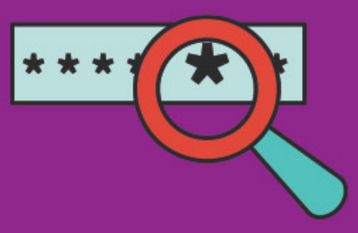
Svi operacijski sustavi podložni su riziku od zaraze. Ako je dostupno, pazite da koriste rješenje za mobilnu sigurnost koje otkriva i sprječava zlonamjerni i špijunski softver te zlonamjerne aplikacije, uz druge značajke zaštite privatnosti i zaštite od krađe.

INTERNETSKA SIGURNOST DOMA

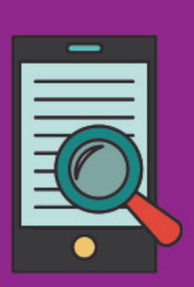
Napravite sigurnosne kopije dokumenata i redovito ažurirajte softver

Instalirajte antivirusni softver na sve uređaje povezane s internetom

Wi-Fi: uvijek promijenite zadanu lozinku za ruter



Koristite jake i različite lozinke za e-mail i račune na društvenim mrežama



Provjerite dozvole za aplikacije i izbrišite one koje ne koristite

Provjerite postavke privatnosti na računima društvenih mreža

Osigurajte elektroničke uređaje lozinkama, PIN-om ili biometrijskim podacima

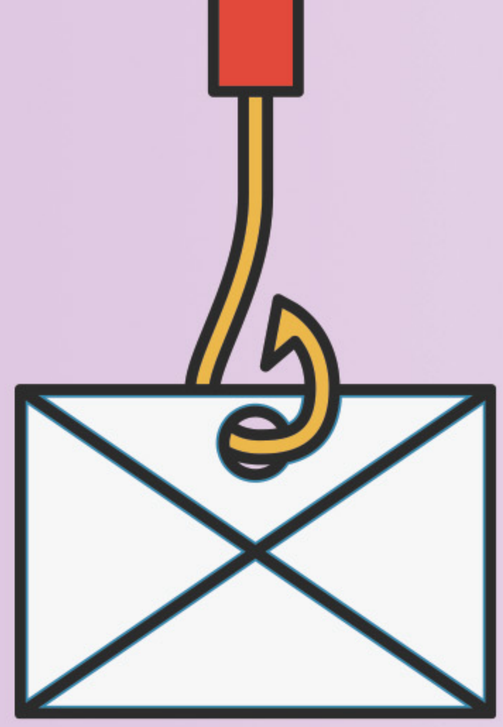
SAVJETI ZA SIGURNU INTERNETSKU KUPNJU

Kupujte od **POUZDANIH** internetskih prodavača i provjerite ocjene

KORISTITE KREDITNE KARTICE ZA ONLINE KUPNJU RADI bolje zaštite

DOBRO RAZMISLITE: ako ponuda zvuči predobro da bi bila istinita, vjerojatno nije

Provjeravajte bankovni račun zbog **SUMNJIVIH AKTIVNOSTI**



BUDITE OPREZNI I **NIKAKO**

- Ne odgovarajte na sumnjive poruke/pozive
- Ne otvarajte poveznice ni privitke u neželjenim e-mailovima/sms-ovima
- Ne dijelite podatke o svojoj bankovnoj kartici ili financijama
- Ne prosljeđujte vijesti iz neslužbenih izvora
- Ne donirajte sredstva humanitarnim organizacijama bez provjere autentičnosti
- Ne kupujte stvari koje su drugdje rasprodane
- Ne šaljite unaprijed novac nepoznatoj osobi

RAČUNALNA SIGURNOST DJECE

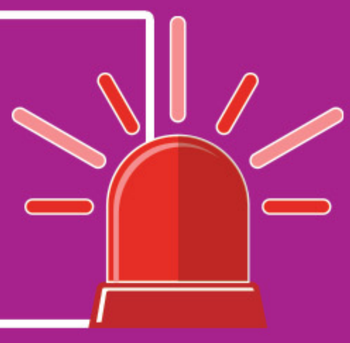
Provjerite postavke **SIGURNOSTI PRIVATNOSTI** pametnih igračaka

Koristite opciju **RODITELJSKOG NADZORA** internetske aktivnosti djece

Promijenite tvorničku **LOZINKU** i redovito ažurirajte softver

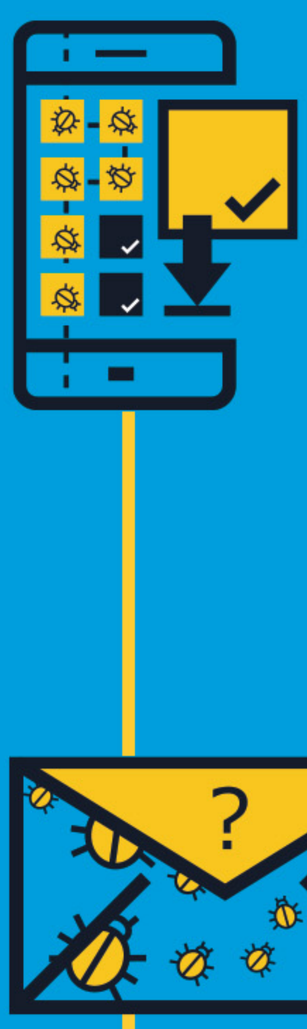
RAZGOVARAJTE s djecom o internetskoj sigurnosti; **SLUŠAJTE** njihova iskustva te im **OBJASNITE** važnost sigurnosti na internetu i izvan njega

ZAPAMTITE
Pratite pouzdane izvore i ažurirane činjenice. Ako postanete žrtva računalnog kaznenog djela, prijavite to policiji.



ZLONAMJERNI PROGRAMI ZA MOBILNE UREĐAJE

KORISNI SAVJETI ZA ZAŠTITU



1 INSTALIRAJTE APLIKACIJE SAMO IZ PROVJERENIH IZVORA

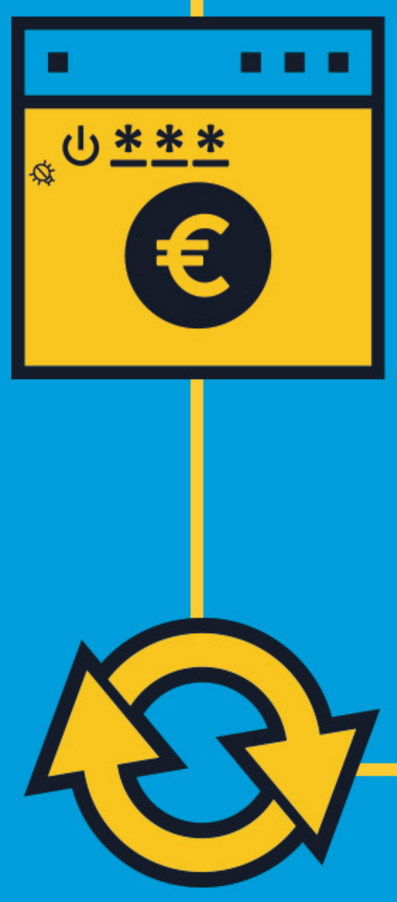
Kupujte u trgovinama aplikacija s dobrim recenzijama – prije preuzimanja aplikacije, istražite i aplikaciju i njezine izdavače. Pazite na web-poveznice koje dobivate u porukama e-pošte i SMS porukama koje vas mogu prevariti da instalirate aplikacije treće strane ili iz nepoznatih izvora.
Provjerite recenzije i ocjene drugih korisnika ako su dostupne.
Pročitajte dopuštenja aplikacije – provjerite kojim vrstama podataka aplikacija može pristupati te dijeli li vaše informacije s vanjskim stranama. Ako ste sumnjičavi oko uvjeta ili vam oni izazivaju nelagodu, nemojte preuzimati aplikaciju.

2 NEMOJTE KLIKATI MREŽNE POVEZNICE ILI PRIVITKE U NEŽELJENIM PORUKAMA E-POŠTE ILI SMS PORUKAMA

Nemojte vjerovati internetskim-poveznicama u neželjenim porukama e-pošte ili u tekstualnim porukama (SMS i MMS) – izbrišite ih čim ih primite.
Dvaput provjerite skraćene URL adrese ili QR kodove – mogli bi vas odvesti na štetna internetska mjesta ili vas navesti da izravno preuzmete zlonamjerni softver na svoj uređaj. Prije klika na poveznicu, upotrijebite pretpregled internetske lokacije URL-a kako biste potvrdili da je adresa legitimna. Prije skeniranja QR koda, odaberite QR čitač koji obavlja pretpregled ugrađenih internetskih adresa te koristi softver za sigurnost mobitela koji vas upozorava na rizične internetske veze.

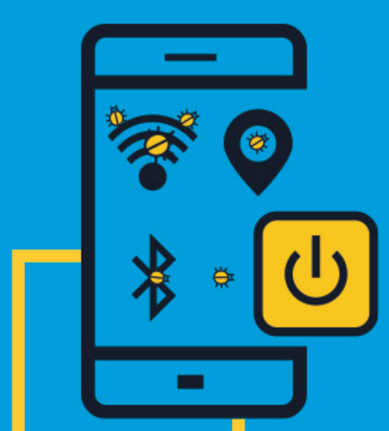
3 ODJAVITE SE S WEB-LOKACIJE NAKON OBAVLJENE KUPNJE

Nikada nemojte korisnička imena i lozinke pohranjivati u mobilnom pregledniku ili u aplikacijama – ako mobilni telefon ili tablet izgubite, svatko se može prijaviti u vaše račune. Nakon završetka transakcije, odjavite se s internetske lokacije umjesto da samo zatvorite preglednik.
Nemojte obavljati bankovne transakcije ili internetske kupnje koristeći javne Wi-Fi veze – mrežno bankarstvo i transakcije koristite samo na mrežama koje poznajete i kojima vjerujete.
Dvaput provjerite URL internetska mjesta – provjerite je li mrežna adresa ispravna prije prijave ili slanja osjetljivih informacija. Preuzmite službene aplikacije banke kako biste bili sigurni da se uvijek povezujete na stvarno internetsko mjesto.



4 AŽURIRAJTE OPERACIJSKI SUSTAV I APLIKACIJE

Preuzmite softverska ažuriranja za operacijski sustav svog mobilnog uređaja čim se to od vas zatraži - najnovija ažuriranja omogućit će veću sigurnost vašeg uređaja i pomoći mu da radi bolje.



5 ISKLJUČITE WI-FI, LOKACIJSKE USLUGE I BLUETOOTH KADA IH NE UPOTREBLJAVATE

Isključite Wi-Fi mrežu kada je ne upotrebljavate – kibernetički kriminalci mogu pristupiti vašim podacima ako veza nije sigurna. Ako je moguće, umjesto povezivanja preko „hotspota“, birajte 3G ili 4G podatkovnu vezu. Možete se odlučiti i za uslugu virtualne privatne mreže (VPN) da bi vaši podaci ostali kriptirani u prijenosu.

Nemojte aplikacijama dopustiti da koriste vaše lokacijske servise ako to nije nužno – ta vrsta informacija može se dijeliti ili „procuriti“ pa koristiti za guranje oglasa na temelju vaše lokacije.

Isključite Bluetooth kada vam nije potreban – pazite da bude posve isključen, a ne samo u nevidljivom načinu rada. Zadane su postavke često unaprijed podešene tako da drugima dopuštaju povezivanje s vašim uređajem bez vašeg znanja. Zlonamjerni korisnici mogu potencijalno kopirati vaše datoteke, pristupiti drugim povezanim uređajima ili čak ostvariti daljinski pristup vašem telefonu kako bi pozivali i slali tekstualne poruke, što za posljedicu ima visoke račune.

6 IZBJEGAVAJTE ODAVANJE OSOBNIH INFORMACIJA

Nikad nemojte odgovarati osobnim informacijama na tekstualne poruke ili poruke e-pošte koje tvrde da dolaze iz vaše banke ili drugog legalnog poslovnog subjekta. Umjesto toga, izravno kontaktirajte taj poslovni subjekt i potvrdite njihov zahtjev.

Redovno pregledavajte svoje račune za mobitel kako biste utvrdili sve sumnjive troškove – ako otkrijete troškove koje niste počinili, odmah se obratite svojem davatelju usluga.

7 NEMOJTE „OTVARATI“ ('JAILBREAK' POSTUPAK) SVOJ UREĐAJ

„Otvaranje“ je postupak uklanjanja sigurnosnih ograničenja koja nameće davatelj operacijskog sustava kako bi se dobio potpun pristup operacijskom sustavu i značajkama. Otvaranje uređaja može znatno oslabiti njegovu sigurnost i otvoriti sigurnosne rupe koje možda nisu bile vidljive.

8 STVARAJTE SIGURNOSNE KOPIJE SVOJIH PODATAKA

Mnogi pametni telefoni i tableti imaju mogućnost bežičnog stvaranja sigurnosnih kopija – provjerite mogućnosti ovisno o operacijskom sustavu svojeg uređaja. Stvarajući sigurnosnu kopiju za svoj pametni telefon ili tablet, možete jednostavno vratiti osobne podatke ako se uređaj ikada izgubi, ukrade ili ošteti.

9 INSTALIRAJTE APLIKACIJU ZA MOBILNU SIGURNOST

Svi operacijski sustavi podložni su riziku od zaraze. Ako je dostupno, koristite rješenje za mobilnu sigurnost koje otkriva i sprječava zlonamjerne programe, špijunski softver i zlonamjerne aplikacije, uz druge značajke zaštite privatnosti i zaštite od krađe.

SIGURAN RAD NA DALJINU

SAVJETI I PREPORUKE

OBAVIJESTITE ZAPOSLENIKE O MOBILNIM RIZICIMA

Mobilni rad zamućuje granicu između poslovne i osobne upotrebe. Tvrtke mogu pretrpjeti golemu štetu napadom koji je inicijalno bio usmjeren na mobilni uređaj pojedinca. Mobilni uređaj je računalo i potrebno ga je zaštititi kao što štitite računala.

OSIGURAJTE SVOJU KORPORATIVNU KOMUNIKACIJU

Provedite upotrebu multifaktorske provjere autentičnosti za pristup korporacijskim računima e-pošte. Omogućite pristup sigurnim komunikacijskim kanalima za zaposlenike radi lakog međusobnog povezivanja te komunikacije s vanjskim suradnicima.

OSIGURAJTE SVOJU OPREMU ZA RAD NA DALJINU

Primijenite mjere poput šifriranja tvrdog diska, vremenskih ograničenja neaktivnosti, zaslona privatnosti, jake provjere autentičnosti i kontrole prenosivih medija i enkripcije (npr. USB pogona). Provedite postupak za onemogućavanje pristupa na daljinu izgubljenom ili ukradenom uređaju.

POVEĆAJTE NADZOR SIGURNOSTI

Aktivno provjeravajte neobične aktivnosti udaljenog korisnika i povećajte razinu upozorenja za napade povezane s VPN-om.

SIGURAN PRISTUP NA DALJINU

Omogućite samo svojim zaposlenicima da se povežu s korporativnom mrežom putem VPN-a koji pruža tvrtka s višefaktornom autentifikacijom. Osigurajte automatski istek vremena rada na daljinu i traženje ponovne provjere autentičnosti nakon određenog razdoblja neaktivnosti.

POVEĆAJTE SVIJEST OSOBLJA O RIZICIMA RADA NA DALJINU

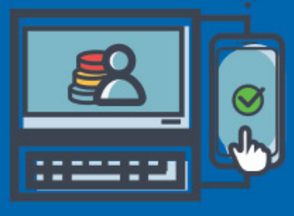
Educirajte zaposlenike o politici tvrtke na području rada na daljinu. Odvojite vrijeme za podizanje svijesti o kibernetičkim prijetnjama, posebno o phishingu i socijalnom inženjeringu.

REDOVITO AŽURIRAJTE OPERATIVNE SUSTAVE I APLIKACIJE UREĐAJA

To će pomoći u smanjenju rizika od kibernetičkog kriminala u kojem se iskorištavaju ranjivosti za koje nema zakrpa.

REDOVITO SE JAVLJAJTE OSOBLJU

Postavite realne ciljeve, raspored rada i mehanizme daljnjeg praćenja, budite fleksibilni gdje je to moguće i uzmite u obzir osobne okolnosti.



PRISTUPITE PODACIMA TVRTKE PREKO OPREME TVRTKE

Koristite samo uređaje i softver koji tvrtka stavlja na raspolaganje. Stvorite snažne lozinke (koristite pouzdane/odobrene upravitelje lozinki ako su dostupni), ne zapisujte ih i zaštitite ih od pogleda prilikom unošenja. Izbjegavajte mogućnosti zaobilaznih rješenja, čak i ako vam se čini da pružaju upravo ono što vam je potrebno.

BUDITE NA OPREZU

Pazite na sumnjive aktivnosti i zahtjeve, posebno one financijske prirode. To bi mogla biti CEO prijevara! U slučaju sumnje, nazovite podnositelja zahtjeva radi dvostruke provjere.
Ne otvarajte poveznice ili privitke primljene u nezatraženoj e-pošti i tekstualnim porukama.

STANITE, PROMISLITE, SPOJITE SE

Prije nego što započnete rad na daljinu, upoznajte se sa službenim uređajima, pravilima i postupcima. Pazite da razumijete kako radi oprema, što se smije, a što se ne smije raditi s njom i gdje potražiti pomoć.

IZBJEGAVAJTE DAVANJE OSOBNIH PODATAKA

Nikada ne odgovarajte osobnim podacima na poruke, čak i ako tvrde da su iz zakonitih izvora. Umjesto toga, kontaktirajte tvrtku izravno kako biste potvrdili njihov zahtjev.

SIGURAN PRISTUP NA DALJINU

Povežite se s korporativnom mrežom samo putem korporativnog VPN-a i zaštitite tokene (npr. pametne kartice) potrebne za VPN vezu.

RAZVIJAJTE NOVE RUTINE

Razgovarajte o planovima rada s vašim izravnim rukovodstvom i članovima tima tijekom rada na daljinu, uključujući raspodjelu zadataka, rokova i kanala komunikacije.

ZAŠTITITE SVOJU OPREMU ZA RAD NA DALJINU I OKRUŽENJE

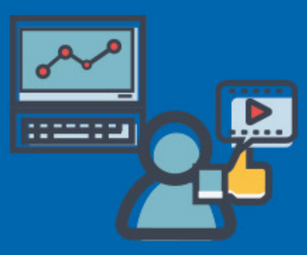
Ne dopustite članovima obitelji pristup vašim radnim uređajima. Zaključajte ih ili isključite kada nisu pod nadzorom i držite ih na sigurnom mjestu da biste spriječili gubitak, oštećenje ili krađu. Spriječite surfanje preko ramena korištenjem zaslona privatnosti i izbjegavajte usmjeravanje zaslona prema prozorima ili kamerama.

UPOTREBA PRIVATNIH UREĐAJA

Ako je korištenje vašeg osobnog uređaja jedina opcija, a poslodavac to dopušta, provjerite jesu li operativni sustav i softver vašeg uređaja ažurirani, uključujući antivirusni/antimalware program i je li veza zaštićena putem VPN-a koji je odobrila vaša tvrtka.

PRIJAVA

Ako primijetite bilo kakvu neobičnu ili sumnjivu aktivnost na bilo kojem uređaju koji koristite za rad na mreži, odmah se obratite svom poslodavcu preko odgovarajućih kanala.



ODVOJITE POSAO OD SLOBODNOG VREMENA

Izbjegavajte osobnu upotrebu uređaja za rad na daljinu.

DVAPUT PROVJERITE PRIJE NEGO ŠTO KLIKNETE

PRIJETNJE S INTERNETA

Mogli biste izgubiti novac, osobne informacije pa čak i pohranjene podatke ako uređaj prestane raditi. Ne dajte se navući!

KAKO SE TO MOŽE DOGODITI?

NAPADI KRAĐOM IDENTITETA: Prijevare korisnika da im oda osobne informacije pretvarajući se da su entitet od povjerenja. Šire se porukama e-pošte, SMS porukama ili platformama društvenih mreža.

PREGLEDAVANJE INTERNETA: Vaš se uređaj može zaraziti jednostavnim posjetom nesigurnoj internetskoj adresi.

PREUZIMANJE DATOTEKA: Zlonamjerne poveznice i privici mogu biti ugrađeni u poruku e-pošte.

ZAŠTO JE UČINKOVITO?

Mobilni uređaji neprekidno su spojeni na internet.

SMANJENA VELIČINA ZASLONA UREĐAJA općenito je ograničenje. Mobilni preglednici prikazuju URL adrese na ograničenom prostoru zaslona, zbog čega je teško vidjeti je li domena stvarna.

Korisnik **IMPLICITNO VJERUJE** u osobnu prirodu mobilnog uređaja.

ŠTO MOŽETE UČINITI?

Budite sumnjičavi ako dobijete SMS poruku ili poziv od tvrtke koja traži vaše osobne informacije. Možete potvrditi legalnost poruke/poziva izravnim pozivom tvrtki na službeni broj.

https://

Kada pregledavate internet s mobilnog uređaja, pazite da je vaša veza sigurna zahvaljujući HTTPS protokolu. Uvijek provjerite nalazi li se na početku URL adrese.

Nikad nemojte klikati poveznicu/privitak u neželjenoj poruci e-pošte ili SMS poruci. Odmah ih izbrišite.

^BE:%}
W@RY
*)Z#$=

Budite oprezni ako završite na internetskoj stranici na kojoj su vidljivi loša gramatika, pravopis ili niska razlučivost.

Ako je dostupna, instalirajte aplikaciju za mobilnu sigurnost koja će vas upozoriti na svaku sumnjivu aktivnost.

WEB HEROJ_

Financira
Europska unija
NextGenerationEU

RH MUP

POLICIJA
RH MUP