SIGURNA KNJIŽICA

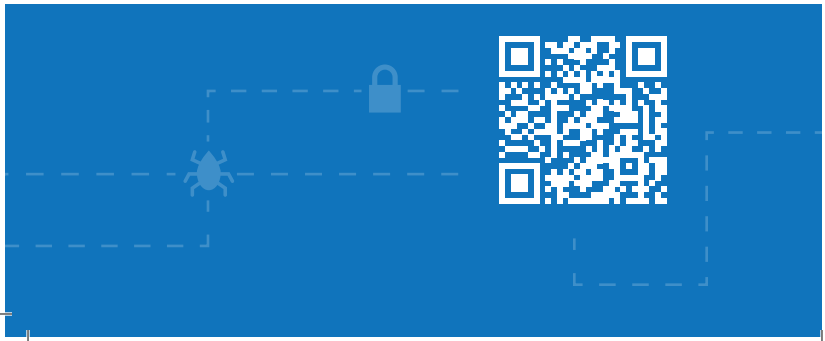
O SVEMU PO MALO

CARNET
znanje povezuje

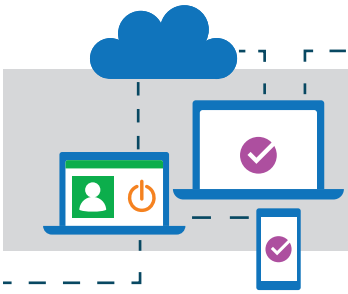
CERT.hr
surfaj sigurnije

ZAŠTO OVA KNJIŽICA ??

- Skup osnovnih informacija za podizanje svijesti i edukaciju o kibernetičkoj sigurnosti na jednom mjestu.
- Zaštita digitalnog identiteta postala je jednako važna kao i čuvanje najvrjednijih osobnih stvari.
- Prikaz osnovnih tema od poznatih kibernetičkih prijetnji do načina zaštite.
- Igrifikacija za promociju kibernetičke sigurnosti u obrazovnom okruženju.
- QR kodovi vode do dodatnih informacija u digitalnom obliku.
- Posjeti internet stranice Nacionalnog CERT-a i edukativne dokumente koji ti mogu pomoći u svakodnevnom radu i u zaštiti vlastitog digitalnog identiteta.



PRIJE SVEGA - BACKUP !!



PODACI VRIJEDE VIŠE
OD UREĐAJA NA KOJEM
SU POHRANJENI!

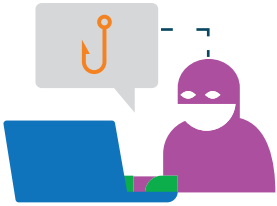
Sigurnosna kopija omogućava povrat podataka u situacijama kada je uređaj na kojem se podaci nalaze izgubljen, oštećen ili ukraden.

Napravi najmanje jednu sigurnosnu kopiju!

Ako možeš, slijedi pravilo **3, 2, 1**!

„Izradi **tri** kopije podataka, od čega su **dvije** pohranjene na istoj lokaciji, ali na različitim uređajima, a **jedna** na skroz drugoj lokaciji."

PHISHING



Phishing je vrsta napada u kojem se pojedinca, lažnim predstavljanjem i naizgled legitimnim zahtjevom, navodi na odavanje povjerljivih podataka ili pokretanje zlonamjernog programa.

Prevaranti postaju sve maštovitiji i izmišljaju nove tehnike phishinga. Obrati pažnju na sljedeće:

Prevaranti često skraćuju poveznice kako bi prekrili stvarnu adresu. Naiđeš li na poveznicu skraćenu pomoću alata **bitly**, jednostavno možeš provjeriti gdje ona vodi dodavanjem znaka plus '**+**' na njezin kraj. Takva poveznica će prikazati pretprikaz ciljanog URL-a.

Bok, mogu li preko tvog broja zatražiti aktivacijski kod za aplikaciju?

NE MOŽEŠ

Ako netko želi pomoću tvog broja mobitela aktivirati aplikaciju, **nemoj na to pristati**! Na taj način osoba se može lažno predstavljati kao ti, ostvariti kontrolu nad tvojim podacima, a tebi onemogućiti pristup.

ZNAKOVI PHISHINGA U DIGITALNOJ KOMUNIKACIJI

LAŽIRANO POLJE POŠILJATELJA

Usporedi prikazano ime i stvarnu adresu e-pošte. Prevaranti se često lažno predstavljaju.

"DRAGI PRIJATELJU"

Općeniti pozdravi, koji nisu upućeni izravno tebi, znak su za oprez.

"POŠALJI MI PODATKE O KARTICI DA TI UPLATIM NOVAC"

Ne dijeli podatke o bankovnoj kartici kao što su: **broj kartice, datum isteka i CVV/CVC broj**.
Za uplatu na račun dovoljan je samo IBAN!

RESET LOZINKE

Ne nasjedaj na ničim izazvan zahtjev za reset lozinke. Prevaranti će te pokušati odvesti na **lažnu formu za prijavu** i tako ti ukrasti podatke.

KLIKNI OVAJ LINK

Ne otvaraj sumnjive linkove već ih provjeri kopiranjem adrese (pomoću desnog klika) u program za uređivanje teksta.

RANSOMWARE - PODACI SU ZAKLJUČANI

Ransomware je naziv za skup zlonamjernih programa koji korisniku onemogućuju korištenje računala. Nakon zaraze *ransomware* može šifrirati datoteke ili onemogućiti korištenje tako da se pojavi početni ekran s određenom porukom koju nije moguće maknuti.

Ransomware je škola koja se skupo plaća!

Broj ransomware napada se udvostručuje iz godine u godinu!

Umanji šansu za ransomware:

1. Ne otvaraj sumnjive privitke iz e-pošte.
2. Ne koristi nepoznate USB stickove.
3. Ne otvaraj sumnjive poveznice.
4. Koristi antivirusni program.
5. Ažuriraj svoje sustave.
6. Datoteke preuzimaj samo iz pouzdanih izvora.

SURFANJE U ANONIMNOM PROZORU

Mnogi misle da ih pretraživanje interneta u anonimnom prozoru preglednika štiti u potpunosti i da nitko ne vidi što su na internetu radili, ali to nije u potpunosti točno.

Anonimno surfanje ne sprema povijest pretraživanja, kolačiće, lozinke i zapis o preuzimanjima lokalno.

Anonimno pretraživanje je korisno prilikom korištenja javnih računala npr. u knjižnici, zbornici, fotokopiraonici i sl.

Pružatelj internetske usluge i dalje može pratiti promet mrežom, a to često mogu i ustanove na čiju mrežu se spaja.

Anonimno pretraživanje ne štiti od hakera, malicioznih programa i drugih izvora opasnosti.

Za sigurno spajanje na bežičnu mrežu provjeri brošuru scanom QR koda.

ŠTO LOZINKU ČINI SNAŽNOM?

DULJINA - barem 16 znakova

RAZNOLIKOST - velika i mala slova, brojevi i znakovi

ORIGINALNOST - bez učestalih fraza 123456, qwertz, asdf

JEDINSTVENOST - svaki sustav treba imati zasebnu lozinku

ANONIMNOST - bez pravih riječi, imena ili značajnih brojeva (datumi)

A što ju čini sigurnom?

Lozinke se ne dijele s drugima niti šalju mailom ili porukama.

Ne zapisuju se na papir, pogotovo ne na vidljivim mjestima.

BONUS SAVJET:
koristi upravitelj za lozinke!

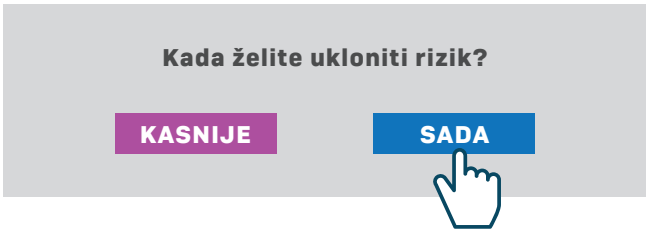
KORAK VIŠE ZA SIGURNOST

Kako sigurnost podataka ne bi ovisila samo o lozinci, preporučljivo je (tamo gdje je moguće) uključiti višefaktorsku autentifikaciju.

ŽURNO AŽURIRANJE

Svakodnevno se otkrivaju veće ili manje ranjivosti raznih operacijskih sustava, softvera i programskih biblioteka. Proizvođači se zbog toga trude pravovremeno uvesti promjene koje uklanjaju ranjivosti kako bi omogućili **žurno ažuriranje** svim korisnicima njihovog proizvoda, time ih štiteći od potencijalnih napada koji iskorištavaju navedenu ranjivost.

Srećom, sustavi većinom daju obavijest o mogućoj nadogradnji sustava, a na nama je samo da to odobrimo kako ne bismo svoj uređaj i podatke izlagali daljnjem riziku.



IGRIFIKACIJA

Igrifikacija zadataka je već dugo poznata u računalnoj sigurnosti te je svojevrstan standard izrade edukativnih materijala, zadataka i izazova pa i certifikacija iz područja računalne sigurnosti. Igrificirani zadaci se u području psihologije smatraju možda i najkvalitetnijim načinom učenja.

Prema mađarskom psihologu Mihalyu Csikszentmihalyu te raznim povijesnim filozofima, igra je "**par excellence**" metoda učenja i jedna od osnova psihologije optimalnog iskustva. Igrifikacija potiče kreativnost, kritičko razmišljanje i pruža užitak učenja kroz igru.

Kao jedan od najboljih primjera igrifikacije su CTF (**Capture The Flag**) zadaci koji su vrlo rašireni u računalno-sigurnosnoj zajednici. U suradnji s **FER-om**, **CARNET**-ov **Nacionalni CERT** svake godine organizira CTF natjecanje **Hacknite** gdje se srednjoškolci natječu u zadacima iz područja sigurnosti kao što su kriptografija, web sigurnost, steganografija, programiranje, reverzni inženjering i razna druga.

Dodatne korisne poveznice:

hackerhighschool.org
picoctf.org
overthewire.org

HACKNITE
CARNET CERT.hr

POVIJEST ČUVANJA TAJNI

Tajne, njihovo čuvanje, a i otkrivanje istih je kroz povijest uvijek bilo od velike važnosti.

SPARTANCI

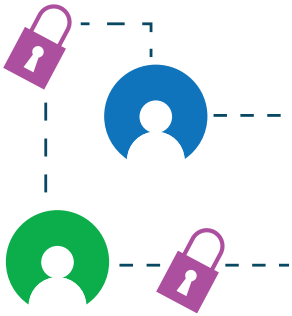
Za prikrivanje tajne poruke Spartanci su koristili **skital**. To je drveni štap oko kojeg se namatala vrpca od pergamenta pa se na nju okomito pisala poruka. Tako bi na odmotanoj vrpci ostali izmiješani znakovi koje je mogao pročitati samo onaj tko je imao štap jednake debljine.

LEONARDO DA VINCI

Kako bi prikrio sadržaj svojih privatnih bilješki Leonardo je koristio skraćeni način pisanja koji je sam osmislio. Za dodatnu zaštitu, poruke je pisao s desna na lijevo tako da su bile čitljive jedino uz pomoć zrcala.

ALAN TURING

U vrijeme Drugog svjetskog rata za šifriranje poruka je korišten sofisticirani kriptografski uređaj Enigma. Turing i tim kriptoanalitičara uspjeli su "probiti" Enigminu šifru te time osigurati stratešku prednost Saveznicima. Svojim radom je zaslužio i naziv oca teorijske računalne znanosti.



KRIPTOGRAFIJA

Kriptografija je jedna od osnova današnjeg interneta te digitalne komunikacije, a koncept je ostao isti od davnina: imamo ključ za šifriranje i ključ za dešifriranje, bilo da se radi o istom ključu ili različitom. Moderna kriptografija se bazira na jačini ključa, dok su algoritmi javno poznati.

Simetrična kriptografija
jedan ključ

Asimetrična kriptografija
par ključeva

Primjeri zadataka

1. ZADATAK #1
Samo najbolji vladari znali su kako sakriti poruku!
FHCDUMHELRMHGDQRGQMLK

2. ZADATAK #2
KAKVE VEZE IMA KEVIN BACON S KRIPTOGRAFIJOM?
AABAB BAAAA AAAAA ABBAA AAABA ABAAA BAAAB

3. ZADATAK #3
KLJUČ OVOG ZADATKA JE CERTHR, A NAJVAŽNIJE JE IGRATI PO PRAVILIMA!
QKFVGBLCIPCLYFMCBDMKHO

Sam pojam **kriptografija** je poprilično apstraktan, ali i jako zanimljiv te se često smatra da je potrebno imati posebno znanje za bavljenje kriptografijom. No, za učenje kriptografije dovoljno je imati osnovno logičko zaključivanje, osnove matematike te pod obavezno - kreativnost. Kriptografija je osnova same računalne sigurnosti i stoga je zastupljena u igrificiranim edukacijskim zadacima iz tog područja.

Trenutno na internetu postoji veliki broj alata, programa i raznih sustava, koji su dostupni besplatno, a omogućuju "preskakanje" ručne kriptoanalize. Primjer takvog alata je **CyberChef** koji koriste i profesionalci.

Do raznih drugih alata možemo doći jednostavnim "**Google oglanjem**", koje se smatra korisnom vještinom u rješavanju igrificiranih zadataka, kako kriptografskih tako i ostalih. Internet je ogromno mjesto i rijetko ćemo se naći u situaciji da smo prva osoba s određenim problemom, stoga nam jednostavna pretraga na internetu može dati vrlo korisne informacije, no **moramo znati što tražimo**.

STEGANOGRAFIJA

Steganografija je metoda skrivanja tajne poruke unutar bezazlenog medija, skupa podataka ili druge poruke čime se prikriva samo postojanje tajne komunikacije.

Jednostavan primjer lingvističke steganografije je **nulta šifra** - definiran set pravila za čitanje poruke, primjerice "čitaj svaki treći znak u svakoj riječi".

VR**T** KR**A**LJA BO**J**ANA
RA**N**O CV**A**TE.

Uz lingvističku postoji i tehnička steganografija koja koristi znanstvene metode za skrivanje poruka, primjerice **nevidljiva tinta**.

Digitalna steganografija uključuje tehnike za skrivanje poruka unutar digitalnih medija. Poruke se tako mogu sakriti unutar neupotrebljenih dijelova datoteka, nealociranog memorijskog prostora ili unutar neiskorištenih dijelova zaglavlja datoteka.

Supstitucija bita najmanje važnosti (LSB)

Kod digitalnih fotografija boje su definirane prema udjelu crvene, zelene i plave boje. Promjenom bita u oktetu koji predstavlja najmanju aritmetičku vrijednost, promjena boje neće biti vidljiva ljudskom oku, ali pregledom bitova najmanje važnosti moći će se iščitati skrivena poruka.

DIGITALNA FORENZIKA

Još jedan od apstraktnih pojmova je digitalna forenzika, za koju čujemo najčešće u CSI serijalu. No, digitalna forenzika bila bi svaka radnja na elektroničkom uređaju kroz koju saznajemo podatke skrivene običnom korisniku, korištenjem raznih programa i metoda, bilo onih koji se nalaze u okruženju operativnog sustava ili rekonstrukcijom izbrisanih i oštećenih podataka.

Digitalna forenzika je odlična **metoda učenja** o računalnim okruženjima i programima koje svakodnevno koristimo, bilo da se radi o proučavanju dobronamjernih ili malicioznih programa. Od jednostavnog nadzora rada programa ili sustava, pa sve do reverznog inženjerstva.

Windows SysInternals je skup besplatnih alata koji se koriste za nadzor, pregled i forenziku Windows operativnog sustava. Koriste se i prilikom računalnih incidenata za jednostavne zahvate, ali i one napredne.

Posjeti i naše velikane hrvatske naive

Godišnji izvještaj nacionalnog Cert-a za 2021. godinu

Pronađite nas na društvenim mrežama

POVEZNICE QR KODOVA

CERT.hr – dokumenti

Sigurnosne kopije

Phishing_članak

Phishing
NCERT-PUBDOC-2018-5-361

Ransomware – plati za svoje podatke
NCERT-PUBDOC-2017-2-346

Sigurnost bežičnih mreža

Savjeti za dobru lozinku

Višefaktorska autentifikacija

Capture The Flag (CTF) natjecanja u području informacijske sigurnosti
CERT.hr-PUBDOC-2019-12-395

Kriptoanaliza
CCERT-PUBDOC-2009-09-275

CyberChef

Steganografija
CCERT-PUBDOC-2006-04-154

Računalna forenzika
NCERT-PUBDOC-2010-05-301

Sysinternals

Naivci.hr

Godišnji izvještaj Nacionalnog CERT-a za 2021. godinu