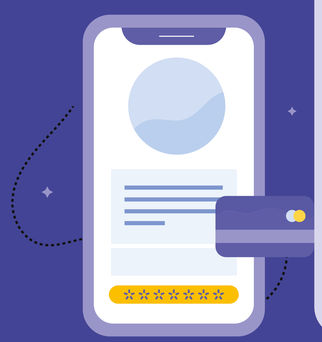
Siguran online život počinje s tobom

Znate li da je financijska šteta od kibernetičkih prijevara 2025. godine u Hrvatskoj bila veća od 20 milijuna eura?

Kako se štete vezane uz kibernetički kriminal na globalnoj razini mjere u bilijunima dolara, kibernetička sigurnost više nije isključiva odgovornost IT sektora već zajednička briga svih sektora društva.

U društvu u kojem se snažno oslanjamo na informacijske tehnologije, pitanja kibernetičke sigurnosti postaju prioritet, i to ne samo za državu i gospodarstvo, već i za građane. I baš zato je sigurnost u tvojim rukama.

Kibernetička sigurnost obuhvaća skup procesa, mjera i standarda kojima se jamči određena razina pouzdanosti pri korištenju proizvoda i usluga u kibernetičkom prostoru



Zakonom o kibernetičkoj sigurnosti uveden je novi, sveobuhvatniji okvir za upravljanje kibernetičkom sigurnošću u Republici Hrvatskoj. Istodobno i Europska unija radi na različitim područjima kako bi promicala kibernetičku otpornost, zaštitila našu komunikaciju i podatke te očuvala sigurnost kibernetičkog prostora i gospodarstva.

digital-strategy.ec.europa.eu

Europe Direct Rijeka

Milutina Barača 62, Rijeka
+385 (0)51 514 156
ed-rijeka@porin.hr
edrijeka.porin.hr
@EuropeDirectRijeka
@ed_rijeka

edrijeka.porin.hr

Izložba se održava uz podršku Grada Rijeke

GRAD RIJEKA

RIJEČKA RAZVOJNA AGENCIJA PORIN
Grad Rijeka

EUROPE DIRECT Rijeka

Izložba je realizirana u suradnji s Nacionalnim CERT-om (CERT.hr), dijelom Hrvatske akademske i istraživačke mreže – CARNET.

CERT.hr je nacionalno tijelo za prevenciju i zaštitu od računalnih ugroza sigurnosti javnih informacijskih sustava u Republici Hrvatskoj čiji je osnovni zadatak obrada računalno-sigurnosnih incidenata s ciljem očuvanja kibernetičke sigurnosti u Republici Hrvatskoj.

CERT.hr surfaj sigurnije

CARNET znanje povezuje

Zlonamjerni softver

*Bok, ja sam **Virus**. Tu sam da bez dopuštenja i putem piratskih programa koje ste preuzeli sa sumnjive stranice napravim darmar na vašem računalu.*

*Bu! Ja sam **Scareware** i lažem da vam je računalo zaraženo. Kad preuzmete antivirusni program koji je lažan počinju pravi problemi.*

*Ja sam **Crimeware** i zapravo sam zlonamjerni kod koji pomaže u obavljanju kriminalnih radnji putem računala. Omiljena mi je krađa identiteta, ucjene i krađa osobnih podataka.*

Internetski kriminal je usko vezan sa zlonamjernim softverom. No, možete se učinkovito zaštititi, i to:

- Zaštitom osobnih informacija
- Osiguranjem svoje WI-FI mreže i brigom o mrežnoj sigurnosti
- Redovitim ažuriranjem softvera
- Korištenjem snažnijih i jedinstvenih lozinki
- Oprezom prilikom preuzimanja sadržaja s interneta

www.cert.hr

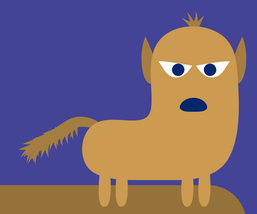
Što nam sve prijeti i kako se zaštititi?

*Ej, ja sam **Keylogger** i baš sam poseban. Namijenjen sam tajnom praćenju i snimanju pritisnutih tipki na računalu. Tu sam da vam ukradem povjerljive podatke poput lozinki za pristup različitim servisima za plaćanje, brojeve kreditnih kartica, PIN-ove...*

*Ciao, ja sam **Spyware**. Kao pravi špijun prikupljam informacije i preuzimam vam kontrolu nad računalom bez vašeg znanja ili dozvole, a za svoju komercijalnu dobit.*

*Ja sam **Rootkit** i posebna sam sorta jer omogućujem napadaču udaljenu administrativnu kontrolu nad računalom. Ponekad je jedini način da me se riješite potpuno brisanje diska i reinstalacija cijelog sustava.*

*Ciao, ja sam zlonamjerni **wiper**, a zovu me i Brisač. Moj je primarni zadatak uništavanje sustava i/ili podataka.*



*Ej, bok, dijelim ime s **Trojanskim konjem** iz mitologije, a lažno se predstavljam kao koristan softver. A kad me instalirate...*

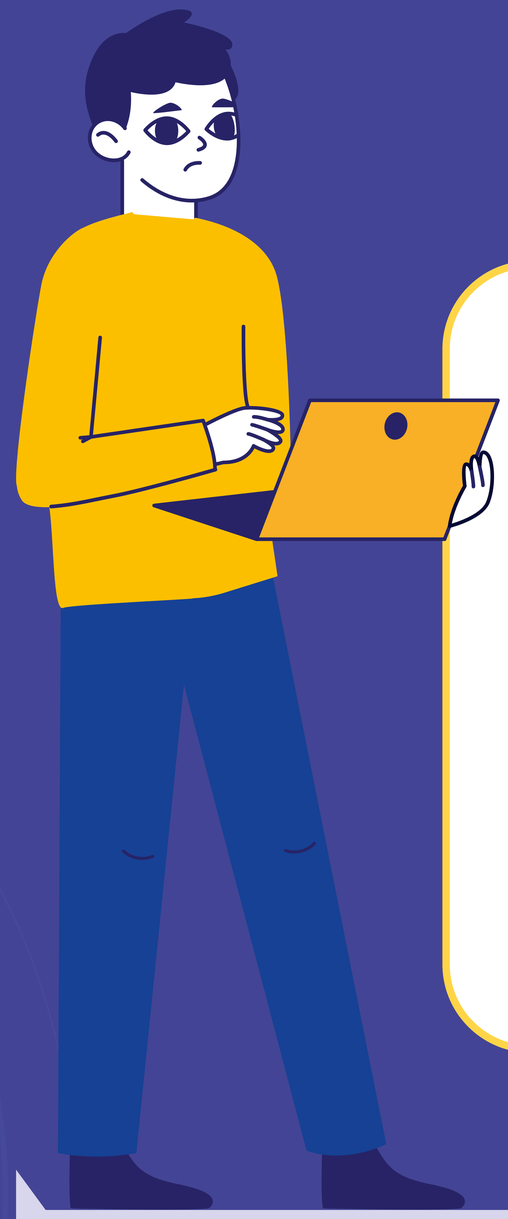
*Mi smo **Crvi** i koristimo računalnu mrežu kako bi s jednog računala zarazili drugo. Koristimo sve nedostatke ili vas lažima i prijevarama pokušavamo nagovoriti na pokretanje kaosa.*

Socijalni inženjering

Osim zlonamjernih softvera, s interneta nam često dolaze prijetnje koje na neki način pokušavaju manipulirati našim odlukama. Te vrste prijevara zajednički se nazivaju socijalni inženjering.

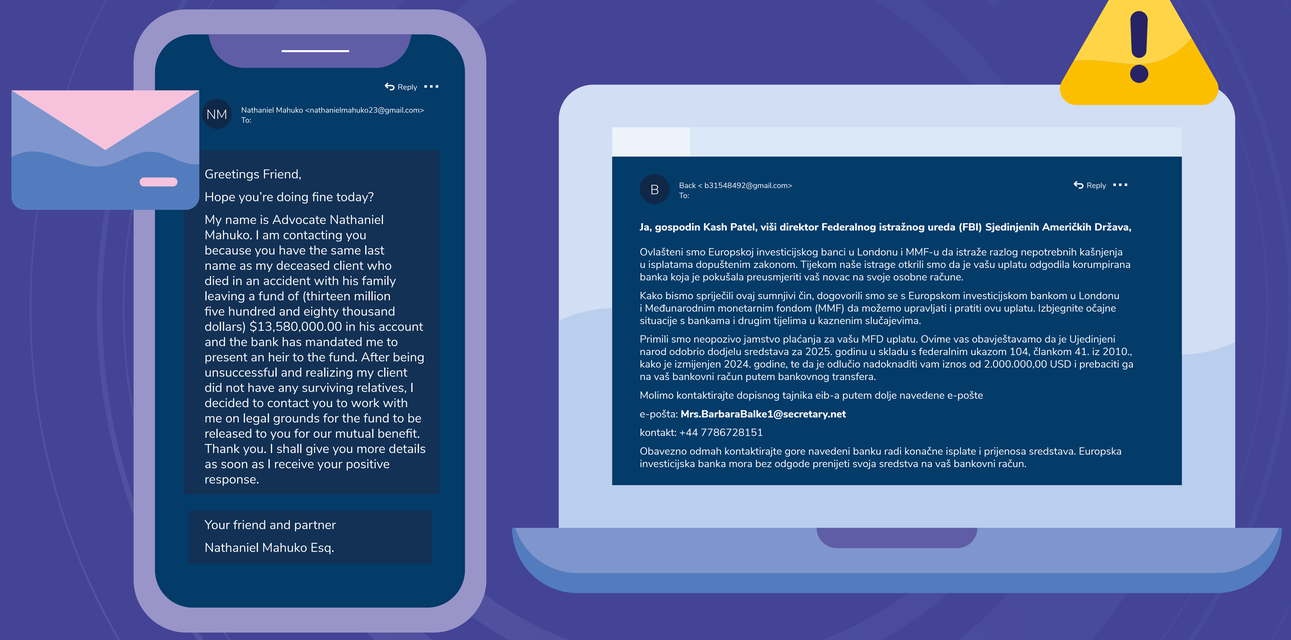
Radi se o manipulaciji ljudima u svrhu otkrivanja povjerljivih informacija ili pristupa resursima do kojih manipulator inače ne može sam doći. U pozadini je uvijek pokušaj da učinimo nešto što nam nije u interesu.

Posljedice uspješno izvedenog napada mogu biti višestruke, a najčešće su materijalni gubitak, gubitak privatnih ili službenih povjerljivih informacija, gubitak ugleda, korištenje podataka za daljnje napade te emocionalni pritisak kojeg osjeća žrtva.



Pazite - većina napada koji koriste socijalni inženjering odvija se u pet faza:

1. ***Sakupljanje informacija o žrtvi***
2. ***Uspostavljanje kontakta sa žrtvom***
3. ***Stjecanje povjerenja***
4. ***Realizacija napada***
5. ***Izvlačenje i brisanje dokaza.***



Kibernetičke incidente možete prijaviti Nacionalnom CERT-u na **incident@cert.hr.**

www.cert.hr/oincprijavi

Kako se ne upecati?

Phishing poruke prenose se putem e-maila, servisa za izravnu komunikaciju (WhatsApp, Messenger, Viber i dr.) ili društvenih mreža. Napadač koristi socijalni inženjering kako bi žrtvu nagnao da napravi nešto što joj nije u interesu.

Zlonamjerni korisnici s tako prikupljenim informacijama mogu u naše ime naručivati proizvode putem interneta, ugovarati usluge, upravljati našim bankovnim računima, a mogu ih iskoristiti i za daljnje napade.

Zapitajte se: ***Kako sam mogao dobiti na lutriji ako uopće nisam uplatio listić? Je li mi mama ikad spomenula rođaka koji je afrički princ? Bi li me banka kontaktirala preko čudne e-mail adrese i tražila osobne podatke?***

Nikada ne odgovarajte na elektroničke poruke koje traže osobne podatke i ne slijedite poveznice koje se nalaze unutar sumnjivih i neočekivanih poruka!

Kako prepoznati phishing

Vishing se odnosi na krađu identiteta putem telefonskih poziva.

Kako prepoznati vishing

Catphishing je vrsta online prijevare u kojoj se počinitelj lažno predstavlja kako bi namamio osobu u odnos ili vezu, s ciljem dobivanja novaca, darova, pažnje ili pristupa osjetljivim informacijama ili resursima.

Kako prepoznati catphishing

Smishing žrtvu cilja putem SMS obavijesti koja sadrži izravnu poruku ili detalj iz lažne narudžbe s poveznicom na lažnu web stranicu.

Društvene mreže

TRI ZLATNA SAVJETA:

1. Postavke sigurnosti i privatnosti postoje s razlogom - držite osobne podatke osobnima. Primjerice, i lokacija je osobni podatak i s njom treba postupati kao i s ostalim osobnim podacima – pažljivo i odgovorno. Provjerite navode li aplikacije koje koristite za što će i kako će koristiti vaše podatke.

2. Održavajte popis prijatelja čistim i zapitajte se poznajete li sve svoje prijatelje/pratitelje.

3. Jednom objavljeno, uvijek objavljeno. Što prije treba osvijestiti kako postupci na društvenim mrežama mogu rezonirati i u stvarnom životu.

Znate li što je Digitalni trag?

Digitalni tragovi

Je li vam hakiran racun

Aktom o digitalnim uslugama Europska unija želi stvoriti sigurnije internetsko okruženje za sve nas. Akt uključuje učinkovito uklanjanje nezakonitog sadržaja i proizvoda, suzbijanje govora mržnja i širenja dezinformacija.

Akt o digitalnim uslugama

Zapamtite, internet ne zaboravlja!

Sigurni online – vodič za djecu i roditelje

Ako se susretneš s nečim neugodnim ili zbunjujućim na internetu, važno je znati da nisi sam/a i da uvijek postoji način da se zaštitiš. Zapamti!

1. **Nije tvoja krivnja** - Nikada nisi kriv/a za nasilje koje ti se događa.
2. **Reci nekome kome vjeruješ** - Ne drži to za sebe — razgovaraj s odraslom osobom kojoj vjeruješ.
3. **Ne odgovaraj na nasilje** - Sačuvaj poruke ili sadržaj i nemoj odgovarati na njih.
4. **Prijavi problem** - Nasilje na internetu prijavi policiji ili odrasloj osobi.
5. **Čuvaj svoje podatke** - Ne dijeli ime, adresu, školu ili broj mobitela s nepoznatima.
6. **Nije ti svatko prijatelj** - Prihvati online prijateljstva samo s ljudima koje poznaješ uživo.
7. **Razmisli prije objave** - Ono što objaviš može utjecati na tvoju budućnost.
8. **Ako ti je neugodno - reagiraj** - Ako se osjećaš loše ili zbunjeno, odmah se obrati nekome.

Potaknite interes svoje djece za tehnologiju i internet, ali usmjeravajte ih da te alate koriste sigurno i odgovorno.

Sigurnost na internetu kao i u životu počinje **razgovorom, povjerenjem i zajedničkom odgovornošću.**

Razgovarajte. Provjerite. Reagirajte. **Budite sigurni zajedno.**

Roditelji, vaša uloga je ključna u zaštiti djece i razumijevanju njihovog online okruženja!

1. **Budite podrška** - Stvorite okruženje u kojem će vam se dijete obratiti bez straha.
2. **Razgovarajte redovito** - Pitajte dijete što radi online i s kim komunicira.
3. **Educirajte o sigurnosti** - Objasnite važnost lozinki, opasnosti linkova i online prijevara.
4. **Postavite pravila** - Odredite dobne granice i pravila korištenja interneta.
5. **Pratite, ali s povjerenjem** - Budite svjesni aktivnosti djeteta, ali gradite odnos povjerenja.
6. **Učite o privatnosti** - Objasnite što su osobni podaci i zašto ih treba štititi.
7. **Razgovarajte o objavama** - Upozorite da online sadržaj ostaje i može utjecati na budućnost.
8. **Reagirajte na vrijeme** - Ako primijetite problem, djelujte smireno i uključite stručnu pomoć ako treba.

Eugen savjetuje

Uključite **automatsko ažuriranje u operacijskom sustavu** i svim aplikacijama kako bi vaši uređaji uvijek imali najnovije sigurnosne zakrpe.

Koristite vatrozid jer on selektivnim propuštanjem prometa izbjegava neovlaštenu komunikaciju i smanjuje mogućnost iskorištavanja sigurnosnih propusta.

Antivirus/antispyware/antimalware su sigurnosna rješenja za prepoznavanje i zaustavljanje aktivnosti zlonamjernog sadržaja.

Koristite složene i različite lozinke - dobra lozinka sastoji se od najmanje 16 znakova!

Budite **oprezni kod online kupnje** - napadači kreiraju lažne internetske trgovine s ciljem krađe novaca i podataka.

Ako nam **bežične mreže nisu ispravno podešene**, omogućavaju svakome u našoj blizini da se u njih uključi. Preporuka je korištenje WPA3 protokola uz AES metodu šifriranja.

Budite oprezni kod korištenja **tuđih pristupnih točaka.** Kada pristupamo nezaštićenoj bežičnoj mreži, sva računala u dometu mogu "preslušavati" informacije koje naše računalo odašilje i prima. Na ovaj način mogu se ukrasti lozinke i drugi važni podaci.

Dvofaktorska ili višefaktorska autentifikacija je sigurnosni proces koji zahtijeva različite metode potvrde identiteta. Ovaj postupak sprječava neovlašteni pristup čak i ako je lozinka kompromitirana. Najčešći faktori autentifikacije su "nešto što poznajete" (lozinka), "nešto što imate" (mobitel) i "nešto što jeste" (biometrija).

Savjeti za dobru lozinku

Nacionalni CERT poziva korisnike da prije online kupovine provjere internetske trgovine na besplatnom servisu iffy.cert.hr koji korisnicima prije ili prilikom online kupovine omogućuje provjeru ima li internetska trgovina obilježja lažnog weba.

iffy.cert.hr

Aktom o kibersigurnosti Europske unije uspostavljen je Europski okvir za kibersigurnosnu certifikaciju, kojim se utvrđuju zajednički kibersigurnosni zahtjevi i kriteriji evaluacije za certifikaciju proizvoda, usluga i procesa.

cybersecurity-act

A što je s umjetnom inteligencijom?

Uz toliko podataka dostupnih na webu i društvenim mrežama, sve je lakše umjetnom inteligencijom stvoriti virtualnu osobu koja zvuči i izgleda kao stvarna osoba i ima pristup velikom broju podataka koje se koriste za provjeru identiteta.

Prevaranti se danas mogu služiti umjetnom inteligencijom za stvaranje lažnih videozapisa, fotografija ili zvukova koji oponašaju nečiji glas (npr. vašeg bankara), lice (npr. slavne osobe) ili pokrete. Primjerice, deepfake tehnologija manipulira video snimkama do te mjere da se savršeno realistično može prikazati događaj koji se nikad nije dogodio.

Zaštita od ovakvih napada nije laka, jer usavršavanjem tehnologije uvjerljivost manipuliranog sadržaja postaje sve veća!

U svijetu u kojem je sve teže razlikovati stvarno od lažnog, Europska unija je donijela pravila za sigurnu i odgovornu uporabu umjetne inteligencije kroz Akt o umjetnoj inteligenciji. Cilj je zaštititi građane i osigurati da tehnologija ostane u službi ljudi.

Akt o umjetnoj inteligenciji

Napadači koriste umjetnu inteligenciju kako bi stvorili sadržaj koji izgleda uvjerljivo i naveli te da napraviš nešto što inače ne bi. Oni ne napadaju tehnologiju. Napadaju tvoje povjerenje.

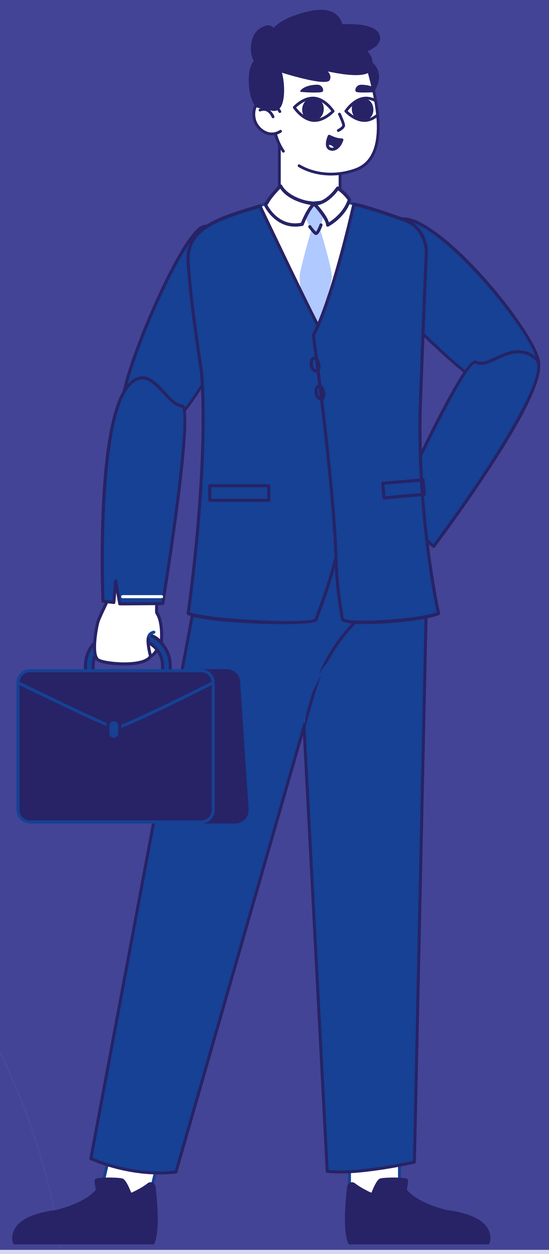
Zato zastani. Provjeri izvor. Razmisli prije klika.

Ne reagiraj na prvu. Ne vjeruj porukama koje stvaraju osjećaj hitnosti ili pritiska. Ako netko traži tvoje podatke ili novac provjeri još jednom, drugim kanalom. Nazovi. Pitaj. Uvjeri se. Jer danas nije dovoljno samo vidjeti. Važno je razumjeti kome i čemu vjeruješ.

Sigurno poslovanje

Kibernetički napadi danas ne ciljaju samo velike poslovne sustave, već sve češće ciljaju na mala i srednja poduzeća. Jedan zaraženi privitak, lažna poruka ili ukradena lozinka mogu dovesti do gubitka podataka, financijske štete, dugotrajnih prekida u radu i štete ugledu.

Napadnutim tvrtkama/organizacijama ponekad je potrebno nekoliko mjeseci za oporavak i ponovni povratak redovnim procesima, uz dodatno financijsko opterećenje gubitka klijenata kao rezultata kibernetičkog napada.



1. *Procijenite slabosti u vašim procesima, a zatim procijenite razinu kibernetičke prijetnje.*
2. *Educirajte sve članove tima - zaposlenici su prva linija obrane. Zaposlenici su najčešća ulazna točka za napade.*
3. *Provodite periodička sigurnosna testiranja.*
4. *Koristite sveobuhvatan pristup kibernetičkoj sigurnosti koji odgovara specifičnostima vašeg poslovanja i zahtjevima vaših zaposlenika.*

Kako bi zaštitila poduzeća od kibernetičkih prijetnji, Europska unija djeluje kroz niz mjera - od jačanja suradnje i stručne podrške do uvođenja jasnih pravila za sigurnost. Ključni okvir je NIS2 direktiva, koja postavlja obveze za sigurnost mreža i podataka te jača otpornost poslovanja.

Direktiva NIS 2

10 zlatnih pravila sigurnosti

1. Redovito **ažurirajte operacijski sustav** i sve aplikacije koje dolaze u kontakt sa sadržajima na internetu
2. **Koristite snažnu lozinku** na kućnoj bežičnoj mreži i javne bežične mreže kojima vjerujete
3. Koristite kompleksne lozinke **za pristup servisima** (društvenim mrežama, e-mailu i slično)
4. Uključite **provjeru u 2 koraka (2FA)** gdje god je to moguće.
5. **Sve novčane transakcije**, a posebno rad s elektroničkim bankarstvom, obavljajte s računala koje je najmanje izloženo riziku zaraze
6. Uvijek **sami u internetskom pregledniku** upisujte adresu stranice na kojoj poslujete novcem, ne koristite poveznice iz primljenih poruka
7. Kada primite poruku u kojoj vam se nudi ili se od vas traži nešto neočekivano, **provjerite je li riječ o prijevari**
8. **Čuvajte sigurnosne kopije** najvažnijih podataka i pri povratu sigurnosne kopije provjerite sadržaj antivirusnim alatom
9. Ne ugrađujte u računalo aplikacije **iz nepoznatih i neprovjerenih izvora,** posebno ako se radi o sigurnosnim alatima
10. **Ne isključujte vatrozid i antivirusni alat** i ne ignorirajte njihova upozorenja

Europe Direct Rijeka

Milutina Barača 62, Rijeka
+385 (0)51 514 156
ed-rijeka@porin.hr
edrijeka.porin.hr
@EuropeDirectRijeka
@ed_rijeka

edrijeka.porin.hr

Izložba se održava uz podršku Grada Rijeke

GRAD RIJEKA

RIJEČKA RAZVOJNA AGENCIJA PORIN
Grad Rijeka

EUROPE DIRECT Rijeka

Izložba je realizirana u suradnji s Nacionalnim CERT-om (CERT.hr), dijelom Hrvatske akademske i istraživačke mreže – **CARNET.**

CERT.hr je nacionalno tijelo za prevenciju i zaštitu od računalnih ugroza sigurnosti javnih informacijskih sustava u Republici Hrvatskoj čiji je osnovni zadatak obrada računalno-sigurnosnih incidenata s ciljem očuvanja kibernetičke sigurnosti u Republici Hrvatskoj.

CERT.hr surfaj sigurnije

CARNET znanje povezuje