Erasmus+
Enriqueciendo vidas, abriendo mentes.

Cofinanciado por el programa Erasmus+ de la Unión Europea

FINALNI DOKUMENT PROJEKTA

Informatička bezbednost u civilnom sektoru

2020-2022

2020-3-ES02-KA205-016585

Federación de Asociaciones de Personas con discapacidad
ORETANIA Ciudad Real

social hackers academy

SADRŽAJ

Erasmus+
Enriqueciendo vidas, abriendo mentes.

Cofinanciado por el programa Erasmus+ de la Unión Europea

Safety in Third Sector

2020-3-ES02-KA205-016585

Istraživanje u okviru projekta Informatička bezbednost u civilnom sektoru (ref. br. 2020-3-ES02-KA205-016585), sufinansiranog od strane Evropske komisije kroz program Erazmus+, sprovedeno je od 11. novembra do 1. januara 2022. godine.

Za potrebe istraživanja sproveden je onlajn upitnik (pomoću aplikacije Google Forms) koji se sastojao od 20 pitanja podeljenih u pet kategorija.

Prva kategorija (šest pitanja) odnosila se na socio-demografske karakteristike organizacija koje su učestvovale u istraživanju, dok su se druga pitanja odnosila na poznavanje zakona o informacijama i elektronskoj trgovini (četiri pitanja), praktični alati (pet pitanja), dobre prakse (dva pitanja) i zaštita podataka nakon Covid-19 (tri pitanja).

UVOD

"STS: Safety in Third Sector" (Informatička bezbednost u civilnom sektoru) je projekat u okviru programa Erazmus+ koji sufinansira Evropska komisija, a koji se bavi analizom, razmenom i promocijom iskustava i dobrih praksi u oblasti sajber bezbednosti i računarske bezbednosti u organizacijama koje rade u društvenom i omladinskom okviru.

Projekat se sastoji od strateškog povezivanja vezanih za za razmenu primera dobrih praksi u oblasti bezbednosti za organizacije u civilnom sektoru. Realizovaće se analize koje će biti predstavljene u vodiču gde se govori o aspektima procene kako bi se osnažili evropski omladinski subjekti koji će da poboljšaju svoju bezbednost prilagođenu raznovrsnosti njihovih potreba.

Cilj je da ojačamo kompetencije naših organizacija donoseći im nove veštine za razvoj boljeg sistema kvaliteta u njihovim uslugama.

Ciljevi ovog projekta su:

- Omogućiti društvenim i omladinskim organizacijama da unaprede svoje veštine u tehnološkom okviru.
- Ojačati saradnju između organizacija u cilju uspostavljanja razmene dobrih praksi.
- Osnažiti omladinske i društvene organizacije da neguju preduzetnički način razmišljanja i veštine kvalitativnog sistema.

Zemlje partneri su: Srbija, Grčka i Španija,

Učesnici uključeni u projekat su
➔ Radnici iz organizacija u kojima učestvuju mladi sa ili bez invaliditeta

UČEŠĆE NEPARTNERSKIH SUBJEKATA:

Biće uključena još dva različita subjekta koji rade sa mladima po zemlji.

AKTIVNOSTI koje će se razvijati zasnivaće se na PROUČAVANJU, ANALIZI i ODREĐIVANJU bezbednih digitalnih alata.

Pored toga, organizovaćemo aktivnost pod nazivom „Bezbednost u našim organizacijama“, koja se sastoji od trodnevnog treninga u kojoj će se sprovoditi obuka za pravilnu primenu stečenih znanja.

INFORMATIČKA BEZBEDNOST U CIVILNOM SEKTORU

UPITNIK

Zahvaljujući partnerima Social Hackers Academy, Sportsko dijagnostičkom centru Šabac i Oretania CR, nakon prikupljanja pravila i primera dobre prakse u sajber bezbednosti, napravili smo test za proveru mera koje se uzimaju u obzir u našim organizacijama da bi bile bezbedne.

Law

Let's talk about our knowledges about the Law regarding to the Information and Electronic Commerce

Do you know and respect the "EU Cookie Laws" *

Practical Tools

Here we would like to know a little bit more about which kind of tools do you use to keep your data protected.

Do you use any kind of program to record/register your actions? *

Good Practices

Here we would like to know if you know good practices regarding to the Security

Do you consider that your organization follow any kind of system (digital or not digital) or good practices to keep your information safe? *

Data Protection after COVID- 19

Year 2020 have been a change in our lives and our organizations and we have changed our procedures after being more used to do everything through a screen... Did it change your work?

Have your organization modified the actions or strategies regarding to the Data Protection after COVID 19?

ANALIZA ISTRAŽIVANJA

REZULTATI

Od ukupno 44 organizacije koje su učestvovale u istraživanju, 16 je bilo iz Španije (36%), 13 iz Grčke (30%) i 15 iz Srbije (34%).
Ispitanici su uglavnom bili iz sledećih sektora: socijalna inkluzija, osobe sa invaliditetom, omladinski radnici i ljudi sa različitim vrstama obrazovanja.

Sektor u kojem organizacija radi (N predstavlja određeni broj slučajeva):

- Social inclusion (N = 6)
- Youth (N = 5)
- Charity work (N = 4)
- Disability (N = 2)
- Ecology (N = 2)
- Informal education (N = 2)
- Education (N = 2)
- Culture & art (N = 1)
- Non formal education (N = 2)
- Consultancy (N = 1)
- Formal education (N = 1)
- Non Formal Education, Youth (N = 1)
- Utilities sector (N = 1)
- Social innovation, entrepreneurship, sustainability, community management (N = 1)
- Social inclusion for people with disabilities (N = 1)

- Social inclusion for people with disabilities (N = 1)
- Youth, Non-formal education, Training (N = 1)
- Social Inclusion, Employment, Training, Non Formal Education (N = 1)
- Entrepreneurship (N = 1)
- Mental health and Social Inclusion (N = 1)
- In all sectors which mentioned above (N = 1)
- Rights of children and youth within formal education (N = 1)
- Sustainability (N = 1)
- Vet, YouTh, Adult education (N = 1)
- Social Inclusion and Youth (N = 1)
- Urban policy (N = 1)
- Disabilities,Youth In Action , Employment, Training, Non Formal Education (N = 1)

ANALIZA ISTRAŽIVANJA

Organizacije uključene u istraživanje rade uglavnom sa mladima, zatim svima kojima je potrebna njihova podrška, osobe sa invaliditetom, osobe u riziku od socijalne uključenosti, mentalnog zdravlja itd.

Grupe sa kojima organizacije rade (N predstavlja određeni broj slučajeva):

- Youth (N = 13)
- Anybody who needs our support (N = 6)
- People with disabilities (N = 8)
- Youth, People with disabilities, People in risk of social inclusion (N = 2)
- Youth, Adults (N = 1)
- Young people, entrepreneurs, immigrants and more (N = 1)
- People with mental health issues, victims of violence, Young people (NEETs), people at risk of social exclusion (N = 1)

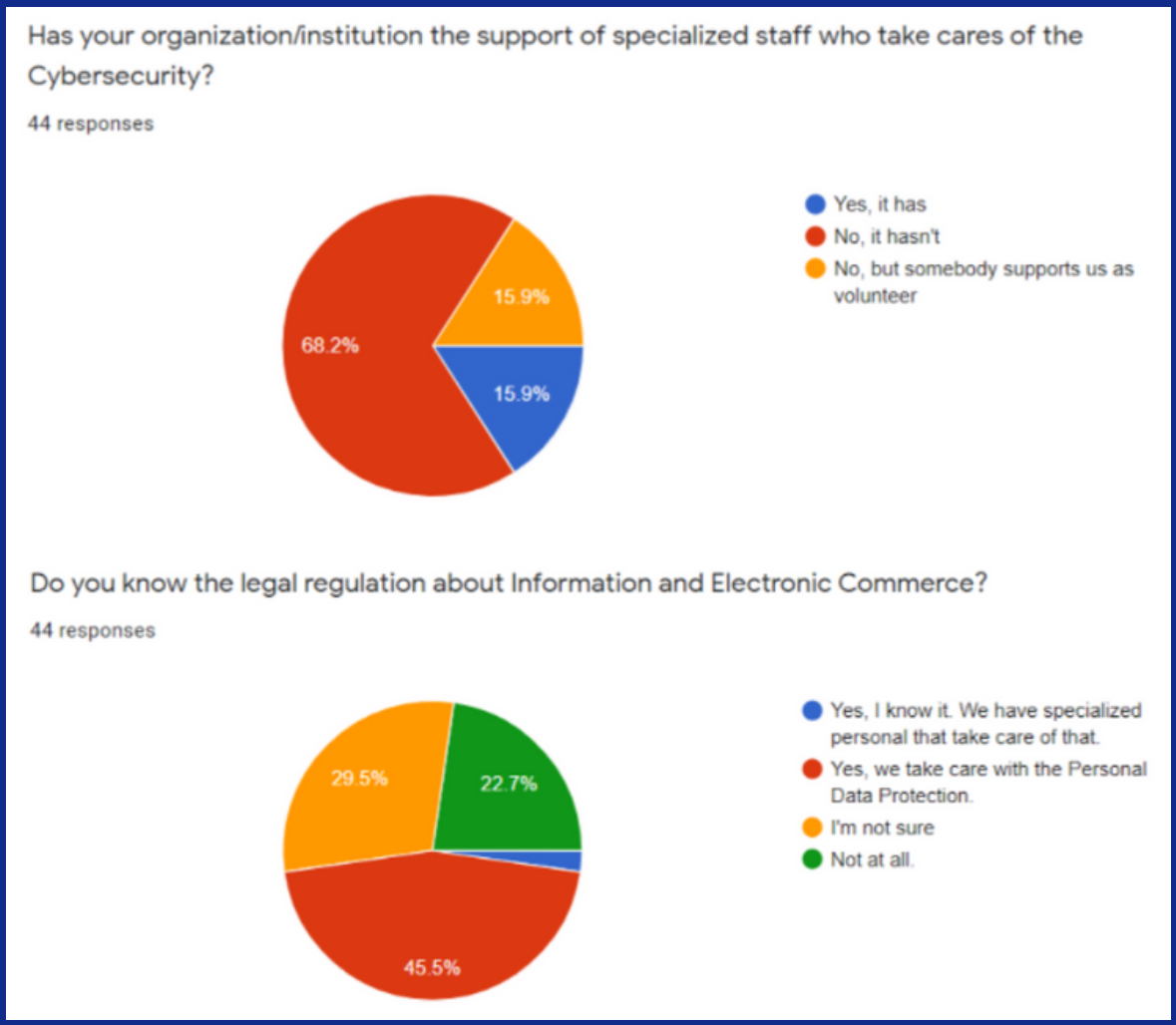
- Children and youth, (un)socially vulnerable, (non)disabled and children and youth at risk of social inclusion (N = 1)
- Eldery, youth, people with mental health issues (N = 1)
- People in risk of social inclusion, Youth (N = 1)
- Women with Endometriosis (chronic illness) (N = 1)
- Youth, vet students, vet teachers, adult learners, adult trainers (N = 1)
- Vulnerable groups, adults (N = 1)
- People with disabilities, elderly, women (N = 1)

- People in risk of social inclusion (N = 1)
- People in risk of social exclusion, young people, migrants/ refugees (N = 1)
- Youth, People in risk of social inclusion, SMEs, Startups (N = 1)
- Youth, Adults and people in risk of social inclusion. There is no limitation about participating in our activities (N = 1)
- Youth, youths with disabilities and adults with education and training courses (N = 1)

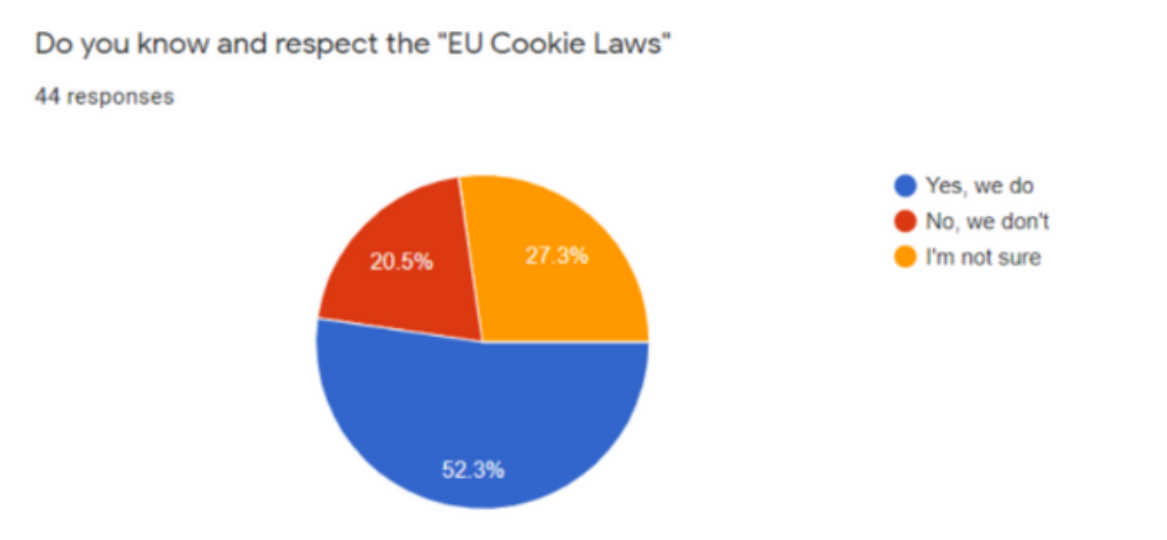
ANALIZA ISTRAŽIVANJA

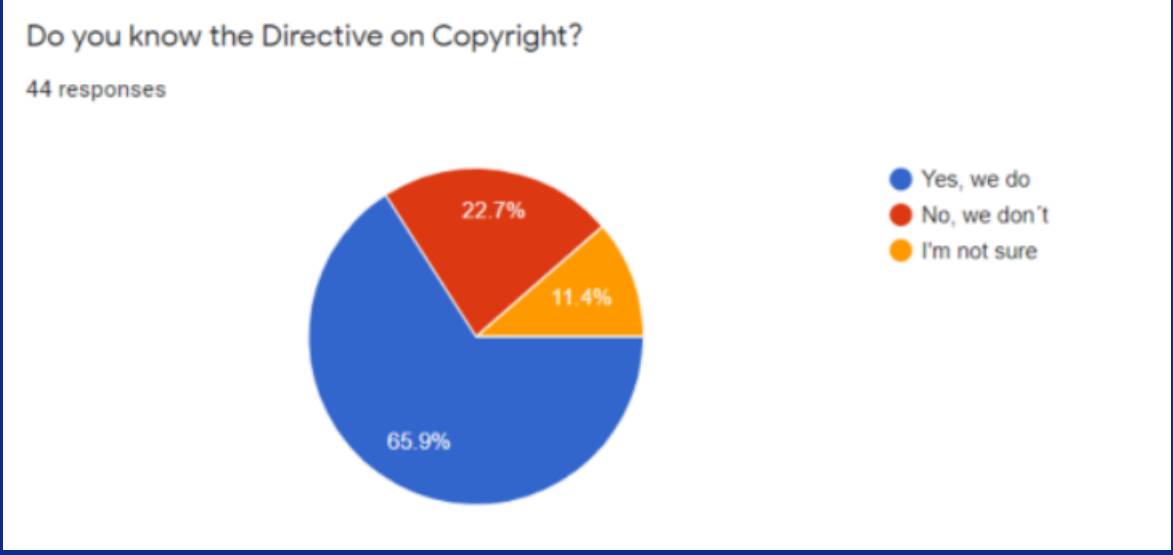
Većina organizacija (55%) ima manje od deset ljudi angažovanih na svom poslu, između 11-50 radi u 32% organizacija i više od 50 ljudi u 14% organizacija. Njihove usluge koristi od 5 do nekoliko hiljada ljudi (u zavisnosti od delatnosti).

Odgovarajući na pitanja o poznavanju Zakona o informisanju i elektronskom poslovanju, ispitanici su odgovorili na sledeći način:



ANALIZA ISTRAŽIVANJA





Kao što se vidi iz grafikona, većina organizacija nema specijalizovano osoblje koje se brine o informatičkoj bezbednosti (68% organizacija), a samo 16% ima nekoga ko će ih na taj način podržati. Ipak, 48% organizacija brine o zaštiti podataka o ličnosti, dok 30% ne zna ili uopšte ne vodi računa (23%).

Iako većina organizacija poštuje zakon EU o kolačićima i poznaje Direktivu o autorskim pravima, postoji veliki procenat onih koji ne znaju ili nisu sigurni u to. Samo 23% organizacija koristi bilo koji program za snimanje/registrovanje svojih akcija.

ANALIZA ISTRAŽIVANJA

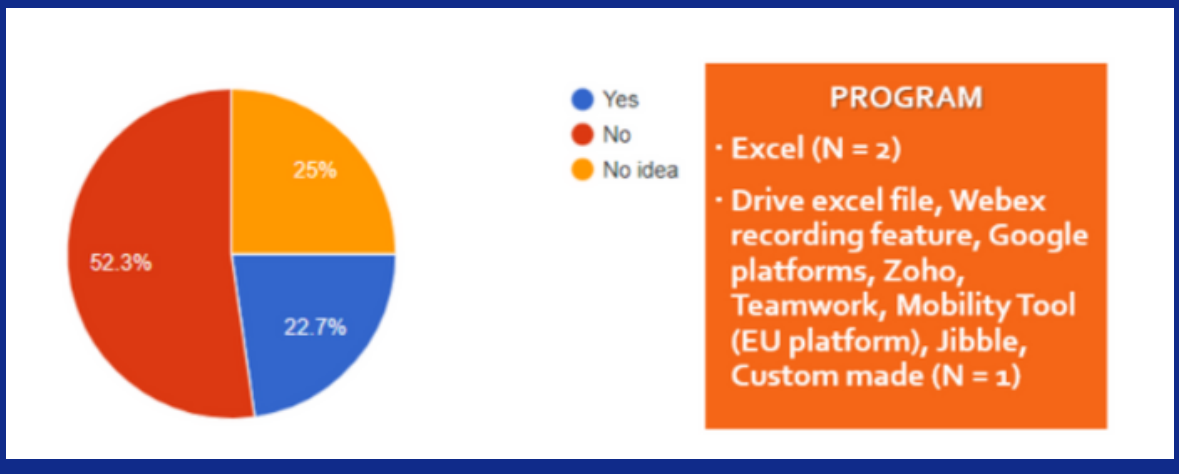
Istovremeno, 59% organizacija koristi bilo koju vrstu programa da bi proverilo da li računar nema zlonamerni softver (uglavnom Avast i Windows Defender), dok 41% ne koristi ili nije siguran na tu temu.

Bilo koji program za upravljanje lozinkama koristi samo 11% organizacija, 78% ne koristi, dok 9% ne zna ništa na tu temu.

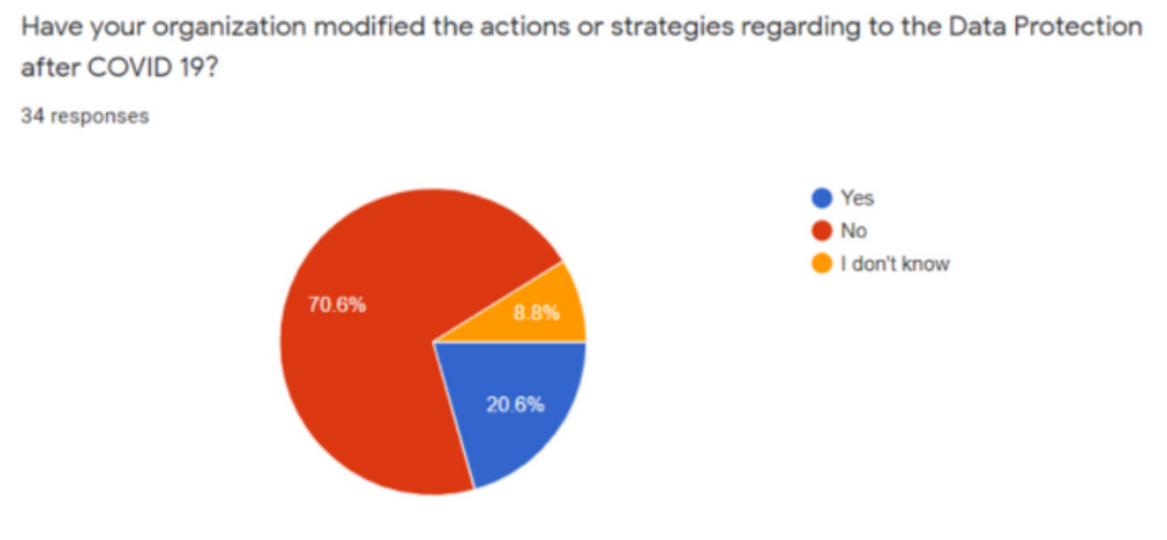
Što se tiče dobrih praksi, većina organizacija (52,3%) ne koristi bilo kakav sistem (digitalni ili ne digitalni) ili dobre prakse da bi svoje informacije zaštitile, a 18% nije sigurno na tu temu.

Organizacije koje su odgovorile DA na prethodno pitanje koriste Cloud, Google Drive, Gmail verifikaciju u tri koraka, rezervne kopije, EU platformu na kojoj je sertifikovana bezbednost podataka, program napravljen po meri ili koriste pomoć eksterne kompanije za zaštitu podataka. Takođe, neki od njih ne koriste iste lozinke u svim servisima i ne čuvaju lozinku u digitalnom formatu (samo na papiru).

Nakon pandemije Covid-19, organizacije uglavnom nisu menjale radnje ili strategije u vezi sa zaštitom podataka, dok je 21% modifikovalo aktivnosti, uglavnom u procedurama.



ANALIZA ISTRAŽIVANJA



Spisak radnji organizacija izmenjenih nakon pandemije kovid-19:

By applying a general security protocol against Covid-19 and specific protocols for each project.
Consent procedures
Procedures
Consent procedures
Procedures
The answer was i don't know
we followed the procedures from Greek National Health Committee for all, organizations and participants (procedures, mobilities and services)
WSe have set more digital tools in order to collaborate together remotely
Change in procedures mainly

ANALIZA ISTRAŽIVANJA

Konačno, poslednje pitanje je bilo „Da li ste prevazišli bilo kakvu poteškoću u vezi sa prinudnom digitalizacijom zbog situacije sa pandemijom“, na koje su ispitanici odgovarali na sledeći način:

No
Yes
/
Adaptation for the use of new forms of communication
We learned some more skills in relation to video calls, digitizing documents ...
Yes, the lack of digital resources
Sort of
We did not digitalise due to pandemic
No because we were already used to work online
I don't know
Both the employees and the parents and legal guardians of the people with disabilities in our organization had to learn how to use the online meeting platforms in order to organize and participate in online lessons such as physical exercise.
We haven't any problem with this. Some off the participants haven't filled the e-forma, just only due negligence or indifference.
Digitalization helped us take our first steps, so it rather worked in our favor.
Yes, more digitalization and we are not well prepared
Not ready
Lack of knowledge on what tools were available out there (mainly free) in order to collaborate closely as a team while working remotely
no difficulty

PRIMERI
DOBRE PRAKSE

PREPORUKE ZA BOLJU BEZBEDNOST

IZ PRIMERA KOJI SU IZNEŠENI NA SASTANCIMA U MADRIDU I ATINI PROIZAŠLE SU SLEDEĆE PREPORUKE

OPREMA:
Rezervne kopije / Cloud.

Za trajno brisanje/korišćenje (Shift-Del) datoteka i za uklanjanje osetljivih podataka.

DELJENJE PODATAKA:
Vodite računa o upravljanju dozvolama kada delite datoteke.

Za šifrovanje ovih elemenata pomoću programa kao što su Winrar ili 7zip.

Da uništite podatke nakon što su već korišćeni (u slučaju da se ne mogu uništiti, preporučuje se da ih čuvate u zaključanim fasciklama).

KORIŠĆENJE INTERNETA:
Kada pretražujete na Internetu, koristite bezbednu veb lokaciju (https://).

Koristite e-poštu isključivo u profesionalne svrhe.

PRIMERI
DOBRE PRAKSE

Proverite primaoca pre slanja pošte.
Preporuka je da to učinite u slepoj kopiji.
Ne šaljite lančane poruke.
Ne odgovarajte na neželjene poruke.

Proverite identitet pošiljaoca pre otvaranja poruke.

Deaktivirajte pregled.

Koristite alate za analizu protiv štetnog koda (virusi, zaštitni zidovi).
Ne otvarajte neželjenu poštu ili sumnjive e-poruke.
Ne otvarajte sumnjive priložene datoteke kao što su Word, Excel, itd., jer mnogi virusi dolaze odatle.
Prijavite mejlove sa virusima, bez prosleđivanja.
Nemojte koristiti poštu kao prostor za skladištenje, jer kada se ono zasiti, unapred uspostavljene usluge pošte mogu prestati da rade.

PRIMERI
DOBRE PRAKSE

LOZINKE:

Moramo da se potrudimo, najbolje što možemo, da naš tim koristi jake lozinke. Ovo uključuje upotrebu malih i velikih slova, brojeva i simbola, kao i to da nikada ne koristite reči koje su na engleskom ili vašem rečniku.

Povremeno menjajte lozinke.

Ne koristite iste lozinke u svim servisima.

Ne čuvati podatke lozinke u digitalnom formatu (na papiru ili šifrovane).

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	1 sec	5 secs
7	Instantly	Instantly	25 secs	1 min	6 mins
8	Instantly	5 secs	22 mins	1 hour	8 hours
9	Instantly	2 mins	19 hours	3 days	3 weeks
10	Instantly	58 mins	1 month	7 months	5 years
11	2 secs	1 day	5 years	41 years	400 years
12	25 secs	3 weeks	300 years	2k years	34k years
13	4 mins	1 year	16k years	100k years	2m years
14	41 mins	51 years	800k years	9m years	200m years
15	6 hours	1k years	43m years	600m years	15 bn years
16	2 days	34k years	2bn years	37bn years	1tn years
17	4 weeks	800k years	100bn years	2tn years	93tn years
18	9 months	23m years	6tn years	100 tn years	7qd years

PRIMERI
DOBRE PRAKSE

1. Uvek koristite Lastpass da delite svoje lozinke sa svojim timom. Ona olakšava uklanjanje pristupa pojedincu kada napusti organizaciju.
2. Koristite Lastpass da kreirate nasumične lozinke i nikada ne koristite istu lozinku iznova i iznova. Čuvajte rezervne kodove negde na sigurnom.
3. Koristite Authi, a NE Google Authenticator kao softver za autentifikaciju sa dva faktora. 2FA treba koristiti apsolutno svuda. Uzdržite se od korišćenja telefona ili e-pošte kao vašeg 2FA sistema. Čuvajte rezervne kodove negde na sigurnom.

PRIMERI
DOBRE PRAKSE

Društvene mreže:

1. Uvek koristite Business Facebook i dodelite pristup samo ljudima koji ga zaista koriste. Kada zaposleni ili volonter ode, obavezno uklonite njihov pristup. Takođe, predlog je da imate samo jednog administratora. Ako date administratorska prava bilo kome, oni mogu da vas uklone za pozicije administratora i mogu dobiti potpuni pristup svim vašim fejsbuk sredstvima, koja uključuju:
   a. Facebook stranicu
   b. Facebook grupu
   c. Instagram stranicu
   d. Nalog za oglase (na početku našeg rada, Fejsbuk nalog našeg suosnivača je hakovan i haker je pokrenuo oglas). Uvek održavajte potrošnju oglasa na niskom.
   e. Fejsbuk Pixels
   f. Itd.
2. Twitter - Koristite 2FA
3. Instagram - Koristite 2FA
4. TikTok - Koristite 2FA

PRIMERI
DOBRE PRAKSE

5. Linkedin - Koristite 2FA na vašem ličnom nalogu, a zatim dajte samo administratorska prava (bez mogućnosti upravljanja korisnicima)

Google Workspace:

1. Primenite obavezno (posle nedelju dana) 2FA pravilo u Google Admin-u. Kada zaposleni ne obrate pažnju na imejl koji im je potreban da bi omogućili 2FA, onda im možete dati 1 od 8 rezervnih kodova.
2. Najnoviji Android uređaji omogućavaju poseban prostor za „Posao“, koji je neophodan za aktivaciju ako želite da koristite svoj profesionalni Gmail nalog i druge Google aplikacije. Standardna Google administratorska prava su malo stroga i zbog toga je predlog da vaš administrator spusti nivo bezbednosti na minimum. Dobra stvar u vezi sa ovom funkcijom je što možete u potpunosti i odjednom da obrišete sve podatke sa telefona vašeg zaposlenog.
3. Ne zaboravite da koristite Authi kao svoj 2FA sistem.

PRIMERI
DOBRE PRAKSE

Osnovno pravilo je da koristite 2FA svuda gde možete.

Morate da napravite rezervnu kopiju SVEGA. To obuhvata:

1. Google Workspace
    a. Calendar
    b. Gmail
    c. Drive
    d. Shared Drives
    e. Bilo šta drugo što vam je važno
2. Alati za komunikaciju (Slack, Discord)
3. Video snimci:
    a. Slack
    b. Vimeo
    c. ltd.
4. Alati za upravljanje projektima (Taskade, Trello)
5. CRM (Airtable, Podio, Salesforce)
6. Aplikacije za beleške:
    a. Evernote
    b. Google Note
    c. Samsung Notes

PRIMERI
DOBRE PRAKSE

Čuvajte svoje tri rezervne kopije odvojeno:

1. Prvu u Cloud programu.
2. Drugu na drugoj Cloud lokaciji.
3. Treću u uređaju za fizičku rezervnu kopiju (poželjno je da držite dve fizičke rezervne kopije na različitim lokacijama).

WordPress:

1. Teška korisnička imena i lozinke sa 2FA.
2. Određene uloge korisnika (dajte što je moguće niže i nadogradite ih samo kada je potrebno). Imajte samo jednog administratora.
3. Omogućite SSL - Hajde da šifrujemo (Let's Encrypt).
4. Investirajte u bezbednu uslugu hostinga (poželjno je da koristite namenski WordPress hosting).
5. Održavajte vaš serverski PHP ažurnim.
6. UVEK ažurirajte (po mogućnosti automatizujte) svoju verziju WordPress-a, WordPress temu (nikada ne koristite besplatnu ili krekovanu temu) i dodatke.

PRIMERI
DOBRE PRAKSE

7. Dodaci (izaberite ih na osnovu kriterijuma)
    a. Sigurnosni dodatak
    b. Ograničeni pokušaji prijave
    c. Sakrivanje stranice za prijavu
    d. Sakrivanje .htaccess datoteke
    e. Premeštanje wp-config datoteke
    f. Koristite “are you a robot” dodatak
8. Onemogućite XML-RPC
9. Sakrijte svoju verziju Wordpress-a
10. Koristite različita korisnička imena i lozinke za:
    a. Hosting nalog
    b. Prijava na Plesk/CPanel
    c. Baza podataka (nemojte koristiti jednostavno ime)
11. Proverite dozvole za datoteke i servere. Uvek dajte minimalna prava pristupa.
12. Onemogućite uređivanje datoteka na kontrolnoj tabli WordPress-a. Po mogućstvu koristite FileZilla.
13. Napravite rezervnu kopiju vaše veb stranice i baze podataka.
14. DDoS zaštita - Cloudflare.

PRIMERI
DOBRE PRAKSE

Dodatno obezbeđenje:

- Nikada ne koristite javni Vaj-faj, posebno „besplatne“ mreže. Nikada ne znate ko stoji iza te mreže.
- Nikada ne prihvatajte Bluetooth, NFC ili bilo koju drugu vrstu veze.
- Koristite VPN za povezivanje na internet.
- UpTimeRobot - Izmerite vreme na mreži vaše veb stranice.

ZAKLJUČCI

Bezbednost u civilnom sektoru je važna tema. Razlog za ovakvo istraživanje je unapređenje zaštite u budućnosti i povećanje svesti o pretnjama IT sektoru. Rezultati opisuju trend da organizacije iz civilnog sektora nisu baš upoznate sa informatičkom bezbednošću i zaštitom podataka.

Što se tiče jednog od ciljeva ovog projekta – razmene dobrih praksi između učesnika, činjenica da neke organizacije vode računa o ovoj temi može pomoći drugim organizacijama da podignu nivo znanja u ovoj oblasti.

Kroz neke odgovore možemo videti šta je dobro, a šta nedostaje. To je ključno u situacijama poput pandemije Covid-19, a posebno izolacije kada smo primorani da većinu svog poslovanja i komunikacije obavljamo onlajn. Istraživanje je suštinski deo projekta koji pomaže da se dobije pun izveštaj o ovoj temi.

PRIZNANJA

Safety in Third Sector

2020-3-ISE2-KA205-015595

HVALA VAM!