REKOMENDACJE DLA ORGANIZACJI POZARZĄDOWYCH

w zakresie odpowiedzialnych działań w sieci

Wypracowane w ramach projektu
Szkoła Odpowiedzialności Cyfrowej NGO - edycja I
(dedykowana organizacjom równościowym)

Iceland
Liechtenstein
Norway
Active citizens fund

INDID
Instytut Dyskursu
i Dialogu

DEMAGOG

SOCNGO
Szkoła Odpowiedzialności Cyfrowej

Autorzy

W ramach modułu „Rzetelność” rekomendacje wypracowywali/ły:

Magdalena Maciejewska, Milena Strehlau, Piotr Ejsmont, Izabella Ferenc, Małgorzata Romanowska, Hanna Shendzer

Mentor: **Filip A. Gołębiewski** (INDID)

W ramach modułu „Prawda” rekomendacje wypracowywali/ły:

Krzysztof Kozicki, Ewelina Lasota, Eugeniusz Kończak, Edyta Czernecka, Dawid Biernat, Jakub Kościółek, Izabella Ferenc

Mentor: **Patryk Zakrzewski** (Demagog)

W ramach modułu „Bezpieczeństwo” rekomendacje wypracowywali/ły:

Mykola Bakhur, Monika Pawlak, Hanna Shendzer, Anna Gierczak, Izabella Ferenc, Eugeniusz Kończak

Mentor: **Patryk Zakrzewski** (Demagog)

W ramach modułu „Twórczość” rekomendacje wypracowywali/ły:

Adam Siger, Jolanta Ratyńska, Katarzyna Pawłowska, Izabella Ferenc, Milena Strehlau, Dawid Biernat, Edyta Czernecka, Cezary Kardasz

Mentor: **Filip A. Gołębiewski** (INDID)

Redakcja:

Filip A. Gołębiewski,
Sara Smyczek-Gołębiewska

Skład i opracowanie graficzne:

Kompot Studio

ISBN 978-83-952071-8-1

Wstęp

Prezentujemy Państwu pierwszą publikację wypracowaną wspólnie przez Uczestników i Uczestniczki projektu *Szkoła Odpowiedzialności Cyfrowej NGO*. Jest to publikacja szczególna, ponieważ zbiera rekomendacje dla organizacji pozarządowych w zakresie odpowiedzialnych działań w sieci. Dedykowana jest ona szczególnie organizacjom walczącym o równe prawa wszystkich ludzi, ale głęboko wierzymy, że wskazówki i sugestie zawarte w tym dokumencie posłużą do wprowadzenia zdrowych nawyków wśród przedstawicieli/ek wszystkich NGOsów, co sprawi, że funkcjonowanie tych podmiotów będzie bardziej rzetelne, oparte na prawdzie, bezpieczniejsze i bardziej twórcze. Jednym słowem: ODPOWIEDZIALNE.

Właśnie to słowo - *odpowiedzialność* - jest naszym zdaniem kluczem dla współczesnego funkcjonowania rozmaitych podmiotów w świecie cyfrowym. Rewolucja internetowa przyniosła ze sobą tyle samo szans i możliwości co zagrożeń i patologii. Nie tylko zresztą dla organizacji pozarządowych, ale także dla administracji publicznej, firm, urzędów, nieformalnych inicjatyw, czy po prostu zwykłych ludzi. Któż z nas nie miewa czasem pokusy, żeby udostępnić prymitywnego mema z przerobionym zdjęciem, tylko dlatego, że wyśmiewa nielubianego przez nas polityka? Któż z nas nie rozważał wzięcia udziału w Facebookowym „quizie", mającym ukryty cel w postaci zbierania o nas danych wrażliwych? Kto z nas nie przymykał oczu na dane i informacje, które nie potwierdzają wyznawanej przez nas wizji rzeczywistości? Kto z nas nie pobrał kiedyś zdjęcia znalezionego w Google i wkleił do swojej prezentacji bez sprawdzania praw autorskich? Któż z nas nie miewa jednego hasła do wszystkich miejsc wymagających logowania? W końcu kto nie był bliski wpisania swojego numeru telefonu na stronie internetowej wątpliwej jakości, tylko po to, żeby skorzystać z *70% zniżek na kursy językowe w woj. X*?

Tysiące tego typu zagrożeń czyhają na użytkowników internetu każdego dnia. Kończą się one nierzadko przejmowaniem kont w mediach społecznościowych lub różnego rodzaju wyłudzeniami, w tym finansowymi. Ludzką rzeczą jest błądzić (oby jak najrzadziej!), jednak organizacje pozarządowe mają na sobie szczególną odpowiedzialność w zakresie tego typu działań. One powinny być w pełni świadome tych niebezpieczeństw i wprowadzać do swoich działań mechanizmy przed nimi chroniące. Nierzadko fundacje czy stowarzyszenia realizując swoje projekty dysponują środkami publicznymi bądź pozyskanymi z grantów/darowizn od podmiotów prywatnych lub darczyńców. Utrata ich poprzez wyłudzenie w sieci mogłaby skutkować ogromnymi problemami dla samej organizacji czy członków zarządu, nie mówiąc o stratach wizerunkowych. Podstawową rolą NGO jest ich zabezpieczenie i sprawienie, że realizacja celów statutowych będzie się odbywać w pełnej zgodności z prawem, także w, często niedocenianej, sferze działań cyfrowych.

Marzy nam się, aby dzięki naszemu projektowi, i wypracowanym w jego ramach publikacjom, NGO-sy stały się przykładem do naśladowania w zakresie odpowiedzialnych działań w sieci. Dlatego liczymy, że ta publikacja nie będzie jedynie teoretycznie przydatną pozycją na długiej liście do przeczytania, ale, że jak najszybciej wpłynie na realne, PRAKTYCZNE działania i procedury w trzecim sektorze. Pierwszy i drugi też oczywiście mogą skorzystać!

Stworzenie ostatecznego kształtu rekomendacji zawartych w niniejszej publikacji wymagało wiele pracy i zaangażowania od Uczestników i Uczestniczek pierwszej edycji SOCNGO. Przeszli oni najpierw cykl szczegółowych szkoleń, po czym włączyli się w proces wypracowywania poniższych rekomendacji. Wielkie brawa i podziękowania należą się zarówno im jak i mentorom wspierającym ich w tym procesie. Publikacja niniejsza jest całkowicie bezpłatna i, naszym skromnym zdaniem, niezwykle cenna. Dlatego czerp z niej Drogi/a Czytelniku/Czytelniczko jak najwięcej i przesyłaj ją gdzie się da. Bo czas na to jest właśnie teraz. Działaj odpowiedzialnie w sieci!

Filip A. Gołębiewski

kierownik projektu
„Szkoła Odpowiedzialności Cyfrowej NGO”

Rekomendacje dla NGO z zakresu:

RZETELNOŚĆ

Organizacja odpowiedzialna

INDID

1

Obszar:

Publikowanie treści

Aby rzetelnie funkcjonować w sieci należy to robić zarówno publikując treści jak i je pozyskując. W pierwszej kolejności prezentujemy rekomendacje w zakresie ich publikowania.

Rekomendacja 1

Unikaj sformułowań mocno nacechowanych emocjonalnie, jeśli chcesz przekazać rzetelną informację

Doprecyzowanie: aby informacja była rzetelna należy stosować jak najmniej przymiotników czy sformułowań oceniających, typu: piękny, wspaniały, beznadziejny, brzydki, itp. Dzięki temu unikniesz zarzutów o stronniczość własnych działań.

Komentarz: jeśli jakiś temat budzi nasze nadzwyczajne zaangażowanie - musimy być nadzwyczaj uważni. Zaangażowanie i udział emocji może spowodować publikowanie niesprawdzonych treści - na przykład zbiórek pieniędzy związanych z bliskim nam tematem. Zbiórki publiczne na takich portalach jak pomagam.pl mogą okazać się oszustwem, żerującym na aktualnych ważkich problemach.

Rekomendacja 2

Publikując treści w sieci unikaj iluzji równowagi argumentów

Doprecyzowanie: jeżeli 99% ekspertów twierdzi, że X, a 1% ekspertów twierdzi, że Y, to nie stawiaj znaku równości między nimi, bo wówczas sprawiasz wrażenie, że X i Y są tak samo prawdopodobne.

Rekomendacja 3

Próbując obalić argument interlokutora nie próbuj obalać argumentu, który nie został przez niego przedstawiony

Komentarz: zjawisko, o którym tu mowa nosi nazwę „sofizmat rozszerzenia".

Link: więcej można przeczytać tu: https://mitynauki.pl/tag/sofizmat-rozszerzenia/

Rekomendacja 4

Zawsze podawaj źródła!

Doprecyzowanie: publikując treści odwołujące się do aktów prawnych wskaż te akty (ustawy, rozporządzenia, itp.) i odwołuj się do nich. Publikując treści odnoszące się do wyników badań, raportów, artykułów naukowych również należy podać źródła.

Rekomendacja 5

Pracując z osobami posługującymi się innymi językami niż polski (np. migrant(k)ami) publikuj tłumaczenia treści na język dla nich zrozumiały

Komentarz: nawet jeżeli tłumaczenie nie będzie perfekcyjne może ono być bardzo pomocne. Należy mieć pewność, że tłumaczenie nie wprowadza w błąd (nie używamy translatorów, jeśli nie możemy zweryfikować poprawności). Mogą pojawić się różne rodzaje niedoskonałości tłumaczeń - tu chodzi o merytoryczne sprawy, a nie o drobiazgi typu „on" „in" itd. Jeśli jest tłumaczenie obejmuje kilka języków, warto na początku artykułu/posta zaznaczyć, jakie języki pojawią się w artykule.

Rekomendacja 6

Przekaz i działania organizacji powinny być transparentne

Komentarz: transparentność to dobra droga do uniknięcia manipulacji i budowania negatywnego wizerunku twojej organizacji. Transparentność buduje zaufanie odbiorcy.

Link: więcej można przeczytać tu: https://businessinsider.com.pl/poradnik-finansowy/transparentnosc-co-to-jest-i-jakie-ma-znaczenie--w-biznesie/qy0e61q

Rekomendacja 7

Kiedy publikujesz treści satyryczne - zaznacz, że jest to satyra

Komentarz: w dobie tzw. post-prawdy trudno czasem odróżnić satyrę bądź przeróbkę zdjęcia dla celów sarkastycznych od prawdziwych przekazów i treści. Dlatego, jeżeli chcesz zastosować satyrę wobec jakiegoś zjawiska/osoby i przerabiasz jakieś zdjęcie, to zaznacz wyraźnie, że zostało to przez Ciebie zrobione dla tych celów, żeby nikt nie pomyślał, że to prawdziwy przekaz. Wystarczy dyskretne ozaznaczenie.

Rekomendacja 8

Promując własne działania nie publikuj postów w grupach, które nie mają związku tematycznego z zagadnieniem

Komentarz: nie spamuj, nie bądź nachalny, publikuj treści w miejscach do tego przeznaczonych tak aby trafić do osób zainteresowanych twoją działalnością. Warto stworzyć tabelę w Google Docs gdzie zaznacza się w jakich grupach, jakie treści i kiedy publikujemy.

Rekomendacja 9

Dajcie się poznać całościowo jako organizacja, stosując różnorodne komunikaty, a nie jedynie propagandowe czy stricte PR-owe

Komentarz: zadbaj o wizerunek swojej organizacji, pokazuj jakie działania podejmujecie, publikuj raporty, informuj o osobach/podmiotach, z którymi współpracuje twoja organizacja, pokaż kim są twoi współpracownicy, jakie mają kompetencje, pokaż historię twojej organizacji.

Rekomendacja 10

Zbyt złożone komunikaty formułuj dwuetapowo: 1. streszczenie (esencja), a następnie 2. link do bardziej szczegółowych i pogłębionych informacji

Doprecyzowanie: większość osób oczekuje prostych i jasnych komunikatów. Jednak część odbiorców potrzebuje szczegółów i detali, dlatego bądź gotowy/a na przygotowanie obu wersji w przypadku bardziej złożonych treści.

Rekomendacja 11

Dostosuj formy komunikacji do odbiorców

Komentarz: poznaj swojego odbiorcę i formułuj treści do niego dostosowane. Inaczej będzie wyglądał komunikat skierowany do młodzieży, a inaczej do seniorów. Unikaj języka niezrozumiałego dla przeciętnego odbiorcy. Możesz posłużyć się https://jasnopis.pl/ aby sprawdzić czy treść nie jest zbyt skomplikowana. Pamiętaj jednak by nie upraszczać języka przekazu do poziomu „prymitywnego” . Stosowany styl i język wypowiedzi także buduje wizerunek organizacji.

Rekomendacja 12

Opracowując dane zagadnienie sięgnij do kilku różnych źródeł, aby uniknąć tzw. efektu „kabiny pogłosowej” lub zamknięcia w „bańce informacyjnej”

Komentarz: „bańka informacyjna” to zjawisko, oparte na serwowaniu użytkownikom informacji, które zostały wcześniej specjalnie przefiltrowane i dopasowane do ich preferencji. Źródło: https://alogic.pl/blog/banka-informacyjna-czym-jest-i-jakie-zagrozenia-ze-soba-niesie. Warto także sięgnąć do kilku źródeł by mieć pewność, że zostały ujęte wszystkie aspekty zagadnienia oraz by poznać odmienną perspektywę. O „kabinach pogłosowych” (ang. *echo chamber*) można poczytać tu: https://dyskursidialog.org/2020/05/11/enklawy-w-facebooikstanie/

Rekomendacja 13

Unikaj publikowania grafik, które mogą przekłamywać przekaz i manipulować odbiorcami

Komentarz: najprostszym przykładem są źle opracowane wykresy, które prezentują prawdziwe wartości liczbowe, ale nieproporcjonalne słupki mające je wizualizować. To typowa manipulacja, mająca na celu wprowadzenie odbiorcy w błąd i zafałszowanie danych w praktyce.

Rekomendacja 14

Nie promuj szkodliwych postaw - bierz odpowiedzialność za to co publikuje Twoja organizacja, bo to może mieć wpływ na innych

Komentarz: uwaga na tzw. „efekt Wertera”, czyli zjawisko znaczącego wzrostu samobójstw spowodowane nagłośnieniem w mediach samobójstwa innej osoby. Przy czym nie chodzi tylko o samobójstwa, ale w ogóle o tragiczne w skutkach schematy złego radzenia sobie z sytuacją osobistą. Miejmy na uwadze, że jeśli opublikujemy informacje, że ktoś, nie radząc sobie ze swoją sytuacją (np. osoby LGBT+), popełnił samobójstwo lub dopuścił się zbrodni, może to bezpośrednio wpłynąć na decyzję osób, które będą się identyfikować z jej/jego sytuacją.

Rekomendacja 15

Nie czuj się zobowiązany do publikacji treści, co do których masz wątpliwości (np. niepewne zbiórki), nawet jeśli prosi o to ktoś, wobec kogo masz dług wdzięczności

Komentarz: jeśli jakaś osoba/organizacja pomogła Ci w jakiejś sprawie, nie musisz czuć się zobowiązanym do publikacji treści, o których publikację prosi owa organizacja, a co do których masz wątpliwości (np. niepewne zbiórki). Oczywiście, nie chodzi o to, by być niewdzięcznym. Chodzi o to, żeby nasze poczucie wdzięczności nie zostało wykorzystane.

Obszar:

Pozyskiwanie treści

Poniższe rekomendacje z zakresu RZETELNOŚĆ dotyczą obszaru pozyskiwania treści z sieci. To ważne, żeby swoje działania opierać w wielu różnych źródłach i danych, które są godne zaufania.

Rekomendacja 16

Szukając treści uważaj na te, które są kryptoreklamą

Komentarz: treści reklamowe powinny być w widoczny sposób oznaczone, aby nie powodowały wrażenia obiektywnej informacji. Jednak czasami zdarza się, że jakaś treść jest kryptoreklamą lub przekazem lobbującym za określonymi rozwiązaniami. .

Rekomendacja 17

Szukając informacji o podmiotach należy korzystać z narzędzi umożliwiających wyszukiwanie danych na ich temat

Komentarz: OSINT to technika dostępna dla wszystkich, zapoznaj się z jego metodami, weyfikuj treści na które trafiasz w sieci, korzystaj z danych administracji publicznej, profesjonalnych publikacji, raportów (np. dane z Krajowego Rejestru Sądowego, które w prosty sposób są dostępne w portalu www.rejestr.io)

Link do źródeł: https://niebezpiecznik.pl/post/osint-bialy-wywiad-czyli-techniki-pozyskiwania-informacji-o-ludziach-i-firmach/ , https://cyberforces.com/osint-bialy-wywiad

Rekomendacja 18

Należy być ostrożnym powielając informacje znalezione w sieci (weryfikacja!)

Komentarz: linkujesz treści? Powołujesz się na informacje znalezione w sieci? Upewnij że są one wiarygodne.

Rekomendacja 19

Prowadząc fanpage warto, co do zasady, odpowiadać na komentarze, które się pojawiają. Odpowiadaj merytorycznie, linkuj wiarygodne źródła, bądź transparentny w swoich działaniach

Komentarz 1: warto wprowadzić spójną politykę zarządzania komentarzami. Prowadząc fanpage powinniśmy dbać by regularnie komunikować się z jego odbiorcami. Należy ustalić zasady reagowania na szkodliwe czy złośliwe komentarze natomiast niewskazany jest brak reakcji na komentarze i pytania. Czasami trzeba niektóre z nich usunąć z widoku publicznego. Nie należy bać się usuwania szkodliwych komentarzy, które zawierają określenia obraźliwe lub poniżej pewnego poziomu (zwłaszcza jeśli brakuje nam zasobów czasowych/osobowych na zajmowanie się tym tematem). Natomiast nie powinno się usuwać komentarzy, które są kulturalne i po prostu wytykają nam błędy lub prezentują odmienną opinię.

Komentarz 2: jeśli komentarze powodują u nas mocną reakcję emocjonalną, warto je zostawić na jakiś czas (kilka godzin, dobę), ponieważ dyskusja w emocjach nie służy merytoryce. Prowadząc merytoryczna dyskusję należy co jakiś czas powiedzieć sobie „a może mój rozmówca ma rację lub trochę racji?" i sprawdzić czy tak nie jest. Nie popadajmy też w pułapkę konsekwencji. Ze swoich słów i twierdzeń można się wycofać, jeśli okażą się nie do końca prawdziwe lub błędne – to żaden wstyd!

Rekomendacja 20

Stwórz w swojej organizacji krótką listę źródeł, którym ufasz i opieraj się na nich, jednak nie zapomnij co jakiś czas jej weryfikować!

Komentarz 1: dobrze rozumiemy, że każdorazowa weryfikacja informacji znalezionej w internecie może być bardzo czasochłonna i męcząca. Dlatego żeby ułatwić sobie codzienną pracę warto poświęcić trochę czasu i zweryfikować kilka źródeł rzetelnej informacji. Mogą to być strony urzędów, fundacji lub inne źródła. Warto co jakiś czas robić aktualizację tej listy.

Komentarz 2: przy doborze źródeł staraj się nie kierować się swoimi osobistymi sympatiami. Zasada podobieństwa sprawia, że bardziej sympatyzujemy ze źródłami, które są nam bliższe. Sprawia też, że może być nam trudniej zauważyć moment, gdy przestaną być rzetelne. Zgodnie z hasłem „dare to be grey", unikajmy źródeł, które mają odpowiedź na wszystkie pytania i „nie mają wątpliwości", zwłaszcza w kontekście prognozowania jakichś trendów. Wypowiedzi przepełnione przekonaniem o słuszności są medialne, ale ich wartość merytoryczna może być bardzo niska (nawet, jeśli zostały wypowiedziane przez ekspertów) - nie ufajmy ślepo autorytetom, bez odzwierciedlenia ich twierdzeń w badaniach.

Polecana książka: Robert Cialdini „Wywieranie wpływu na ludzi"

Rekomendacja 21

Próbuj komunikować się z różnymi środowiskami, żeby uniknąć efektu „bańki informacyjnej”

Komentarz: pamiętajmy, że przekonania i zachowania innych ludzi często wpływają na to, czy dane poglądy lub zachowania uznamy za słuszne (zasada dowodu społecznego). Można w ten sposób paść ofiarą tzw. owczego pędu. Pamiętajmy, że postępowanie innych ludzi, na przykład z naszej bańki informacyjnej, nie może stanowić jedynej podstawy do uznania zjawisk za prawdziwe, warte opisania lub promowania.

Komentarz: opisując jakieś zjawisko we własnych kanałach komunikacji warto korzystać z narzędzi Google Trends, które pokazują jak często i gdzie się mówi na dane tematy.

Rekomendacja 22

Przy wyszukiwaniu informacji unikaj tendencyjnego doboru badań!

Komentarz: chodzi np. o odrzucanie badań, których wyniki nie są spójne z Twoim przekonaniem. Nie warto tego robić. Najlepiej odnaleźć artykuły, które stanowią metaanalizę w danym temacie.

Rekomendacje dla NGO z zakresu:

PRAWDA

Organizacja odpowiedzialna

DEMAGOG

2

Rekomendacja 1

Regularnie pokazuj co robi Twoja organizacja i bądź transparentny. Dzięki temu zminimalizujesz ryzyko wystąpienia kampanii dezinformacyjnej wymierzonej w Twoją organizację

Doprecyzowanie: bądź transparentny w swoich działaniach. Na bieżąco informuj o tym, skąd pozyskujesz środki, na co je przeznaczasz, z kim współpracujesz. Odpowiadaj na pytania merytorycznie, posiłkując się wiarygodnymi źródłami. Publikuj raporty, bądź otwarty na dyskusję, nie pozwól, aby ktoś manipulował informacjami na temat twojej organizacji. Dzięki temu zadbasz o wizerunek organizacji i wzmocnisz jej odporność przed dezinformacją.

Rekomendacja 2

W celu ustalenia prawdziwości zdjęcia skorzystaj ze zmysłu obserwacji i wyszukiwania obrazem

Rozwinięcie: przyjrzyj się zdjęciu, którego wiarygodność próbujesz ustalić. Czasem wystarczy rzut oka, aby dostrzec jakąś przeróbkę bądź fotomontaż – może na to wskazywać np. różna/słaba jakość zdjęcia lub jego części, nienaturalne cienie, deformacje. Jeśli masz wątpliwości, skorzystaj z wyszukiwania obrazem.

Rekomendacja 3

Jeśli chcesz uzyskać precyzyjne wyniki, skorzystaj z operatorów wyszukiwania

Rozwinięcie: zaoszczędź swój czas! Możesz zwiększyć precyzję wyników wyszukiwania, używając w zapytaniu słów i symboli. Do najpopularniejszych operatorów wyszukiwania należą:

- site: do wyszukiwania słów kluczowych na konkretnej stronie internetowej
- filetype: do szukania konkretnych rodzajów plików, jak .pdf czy .xls
- symbol - (minus), aby wyeliminować wyniki zawierające słowo kluczowe poprzedzone tym znakiem.

Linki do źródeł:

- https://support.google.com/websearch/answer/2466433
- https://www.google.pl/intl/pl/help/operators.html

Rekomendacja 4

Jeśli masz wątpliwości, co do prawdziwości cytatu, sprawdź, czy znajdziesz go w identycznej w formie w innym (wiarygodnym) miejscu sieci

Rozwinięcie: w sieci nie zawsze prezentowany jest pierwotny wydźwięk wypowiedzi. Cytaty bywają skracane, zmieniane i mogą nas tym samym wprowadzić w błąd. Skorzystaj z operatora wyszukiwania „...”, aby ustalić pierwotne brzmienie cytatu i upewnić się, czy te słowa rzeczywiście zostały wypowiedziane przez osobę, której są przypisane. Upewnij się też, czy cytat funkcjonuje w pierwotnym kontekście.

Rekomendacja 5

Dzięki pracy organizacji fact-checkingowych możesz w szybki sposób sprawdzić, czy dana treść jest zgodna z rzeczywistością

Rozwinięcie: fact-checking to proces, który ma na celu zweryfikowanie informacji, polegający na dokładnym sprawdzaniu faktów w wiarygodnych źródłach, dokumentach na piśmie lub w formie materiałów audio-wideo, a także w wypowiedziach autorytetów posiadających wiedzę i powszechnie uznaną wiarygodność w dziedzinie, której dotyczy weryfikowana informacja. Celem fact-checkingu jest promowanie prawdziwości i poprawności informacji. Organizacje fact-checkingowe stoją na straży rzetelności i prawdy. Warto korzystać z ich wiedzy i informacji, które zdołały ustalić. Głównym celem organizacji fact-checkingowych jest poprawa jakości debaty publicznej. Przede wszystkim skupiają się na weryfikacji dostępnych publicznie wypowiedzi polityków, urzędników lub innych wpływowych osób.

Linki do wybranych portali fact-checkingowych:

- demagog.org.pl
- konkret24.tvn24.pl
- snopes.com
- sprawdzam.afp.com
- politifact.com
- factcheck.org

Rekomendacja 6

Jeżeli chcesz uniknąć rozpowszechniania fałszywych treści związanych z Twoją działalnością, stale obserwuj portale lokalne oraz tematyczne

Rozwinięcie: częste wpisywanie w wyszukiwarce nazwy naszej organizacji lub tematu nas interesującego kieruje nas do artykułów mogących rozpowszechniać nieprawdziwe informacje. Na portalach lokalnych często pojawiają się komentarze podważające naszą działalność. Monitorując i na bieżąco reagując, możemy powstrzymać rozprzestrzenianie się fałszywych informacji.

Rekomendacja 7

Przygotowując materiały do publikacji, pamiętaj o odnoszeniu się do źródeł oraz dobieraniu odpowiednich obrazów

Rozwinięcie: poza wyszukiwaniem informacji często tworzymy treści. Starajmy się, aby nasz przekaz oparty był o wiarygodne źródła i fakty.

Rekomendacja 8

Korzystając z przeglądarki, nie sugeruj się pierwszym lepszym wynikiem. W razie potrzeby zajrzyj na kolejne strony wyników wyszukiwania

Rozwinięcie: często wyszukując treści, kierujemy się pierwszymi wynikami. Należy jednak pamiętać, że część z nich jest sponsorowana przez organizacje/ firmy, którym zależy na rozpowszechnianiu konkretnego przekazu. Pozostałe wyniki uporządkowane są według kolejności, w jakiej wzbudzają zainteresowanie, lecz nawet to nie gwarantuje, że otrzymamy wyłącznie sprawdzone informacje oparte na faktach.

Linki do źródeł:

- https://developers.google.com/search/docs/beginner/how-search-works?hl=pl

Rekomendacja 9

Fałszywi “eksperci” i autorzy artykułów często brzmią wiarygodnie. Sprawdź autora oraz źródła, na które się powołuje

Rozwinięcie: zwracaj uwagę na autorstwo tekstów publikowanych w Internecie. Oceń, czy autor(ka) ma wystarczające kompetencje lub warsztat, aby podejmować dany temat. Sprawdź, kto podaje dalej informację. Czy jest to portal, który nie pozwoliłby sobie na działanie niezgodne ze standardami dziennikarskimi? Czy portal prezentuje informacje w taki sam sposób, jak inne wiarygodne źródła? W ten sposób można rozpoznać propagandę lub manipulację, stronniczość.

Sam fakt, że ktoś wypowiada się w danym temacie, nie musi oznaczać, że mamy do czynienia z ekspertem. Warto sprawdzić, czy ta osoba ma wystarczające kompetencje, żeby wypowiadać się na dany temat.

Jeśli szukasz odpowiedzi na skomplikowane pytania wymagające wiedzy specjalistycznej, sięgnij po czasopisma branżowe, specjalistyczne, które są postrzegane jako wiarygodne źródła wiedzy w danej dziedzinie.

Rekomendacja 10

Jeśli chcesz mieć pewność co do informacji na temat osób i ich powiązań, skorzystaj z oficjalnych stron

Rozwinięcie: nie buduj swojej opinii na podstawie przypadkowych źródeł. Korzystaj z wielu oficjalnych stron. Skorzystaj z tych samych metod, kiedy próbujesz nawiązać współpracę/chcesz przyjąć darowiznę, ale nie masz pełnej wiedzy na temat danego podmiotu.

Linki do źródeł:

- https://rejestr.io/

Rekomendacja 11

Rozpoznanie „fake news” nie jest łatwe. Korzystaj z narzędzi, dzięki którym szybko zweryfikujesz informacje

Rozwinięcie: korzystaj z wielu narzędzi pomocnych przy weryfikacji informacji. Do wyboru masz wyszukiwanie obrazem, aplikacje sprawdzające, czy zdjęcie nie było edytowane, poklatkowa analiza wideo

W gąszczu informacji i w obliczu kampanii dezinformacyjnych znajomość narzędzi weryfikacji jest podstawą

- Izabella Ferenc, Fundacja Rozwoju Społeczeństwa Informacyjnego

Polecane narzędzia weryfikacji:

Weryfikacja obrazów i wideo:

- wyszukiwanie obrazem: Google, Yandex, TinEye, RevEye; załaduj zdjęcie z urządzenia lub wstaw link do obrazu; ogranicz wynik wyszukiwania (data)
- poklatkowa analiza wideo: InVID Plugin (Chrome i Firefox): https://www.invid-project.eu/tools-and-services/invid-verification-plugin/
- metadane: Jeffrey's Image Metadata Viewer
- fotomontaż: FotoForensics
- analiza trendów: Google Trends
- archiwum Internetu – WaybackMachine: https://archive.org/web/
- powiązania w organizacji: rejestr.io
- wyszukiwanie Tweetów https://www.thoracle.net/

Rekomendacja 12

Nie zostawiaj „fake newsa” samego sobie!

Rozwinięcie: jeśli ktoś prowadzi kampanię dezinformacyjną przeciw twojej organizacji, reaguj! Dementuj, podsyłając wiarygodne linki, informacje. Edukuj, ujawniając błędy, bądź merytoryczny. Odwołuj się do sprawdzonych i oficjalnych źródeł. To najlepszy sposób na przeciwdziałanie fake news, przy czym przekaz musi być klarowny i poparty odpowiednią wiedzą.

Rekomendacja 13

Wiedza to Twoja moc i siła Twojej organizacji. Każdy może łatwo ulec dezinformacji. Zapobiegaj temu, a przy okazji rozwijaj kompetencje swojego zespołu

Rozwinięcie: skorzystaj ze zdobytej wiedzy na temat weryfikowania źródeł i informacji nie tylko w życiu osobistym, ale również w swojej organizacji. Zaproponuj współpracownikom szkolenie, podziel się materiałami. Potraktuj to jako szansę na rozwój kompetencji wewnątrz organizacji. To kompetencje, które potencjalnie mogą Was uchronić przed negatywnymi konsekwencjami nieumyślnego udostępniania czy wykorzystania fałszywych informacji.

Rekomendacja 14

Edukuj! Dziel się wiedzą!

Planując projekty, działania dla beneficjentów Twojej organizacji, postaraj się uwzględnić tematykę weryfikowania informacji/cyfrowego bezpieczeństwa (nawet jeśli nie wprost). Wykorzystuj wszystkie okazje do upowszechniania tej niezwykle istotnej wiedzy.

Rekomendacje dla NGO z zakresu:

BEZPIECZEŃSTWO

Organizacja odpowiedzialna

DEMAGOG

3

Rekomendacja 1

Stosuj zasadę ograniczonego zaufania

Doprecyzowanie: bez względu na to, czy otwierasz załącznik do maila, dokonujesz płatności przez Internet czy przekazujesz dane logowania swojemu współpracownikowi, stosuj zasadę ograniczonego zaufania. Zakładaj mniej optymistyczne scenariusze (np. próbę podszywania się, możliwość przechwycenia wiadomości przez osobę trzecią) i zabezpiecz się na taką ewentualność.

Rekomendacja 2

Pamiętaj o tworzeniu i regularnym aktualizowaniu kopii zapasowych danych gromadzonych w Twojej organizacji

Rozwinięcie: ważnym elementem w pracy w organizacji jest gromadzenie danych i informacji o przeprowadzonych wydarzeniach i zrealizowanych projektach a także przetwarzanie danych osobowych. Wszystkie ważne dokumenty i inne potrzebne materiały przechowuj w postaci kopii zapasowej na osobnych nośnikach typu SSD. Pozwoli Ci to odzyskać pliki w przypadku cyberataku, kradzieży, uszkodzenia nośnika lub innego incydentu. Pamiętaj też o zaszyfrowaniu dysku: ustal skomplikowane hasło, które uniemożliwi osobie postronnej odczytanie danych z dysku.

Możesz też skorzystać z usług chmury (np. iCloud, Dysk Google), czyli serwisu internetowego umożliwiającego tworzenie kopii zapasowej „na bieżąco".

Nie używaj w tym celu pendrive'ów, ponieważ te bywają zawodne.

Dzięki tej wiedzy moje dane są w dobrych rękach dysków zapasowych, nie boję się o bezpieczne jutro

– Hanna Shendzer, Fundacja „U-WORK"

Linki do źródeł:

- https://niebezpiecznik.pl/post/kopia-zapasowa-i-migawki-czyli-przepis-na-backup-idealny/
- https://bit.ly/3pc0pln
- https://support.google.com/android/answer/2819582?hl=pl

Rekomendacja 3

Nie każdy pracownik/wolontariusz organizacji powinien mieć dostęp do wszystkich loginów i haseł!

Rozwinięcie: jeżeli przekazujesz login bądź hasło do jakiejś usługi swoim współpracownikom, pamiętaj, aby przesyłać te dane wieloma kanałami (np. login mailem a hasło SMS-em). Udziel dostępu wyłącznie do niezbędnych danych.

Komentarz: jeżeli Twoja organizacja kończy współpracę z daną osobą, zadbaj o zmianę loginów i haseł, do których dostęp miała ta osoba. Jeżeli korzystacie z usług chmury (np. Dropbox, Dysk Google), zablokuj dostęp do plików tej osobie. Zadbaj o właściwe przekazanie skrzynki mailowej pracownika.

Linki do źródeł:

- https://ug.edu.pl/o-uczelni/uslugi-it/ochrona-danych-osobowych
- https://www.politykabezpieczenstwa.pl/pl/a/jak-zabezpieczyc-firme-przed-kopiowaniem-danych-przez-pracownikow
- https://www.isecure.pl/blog/skrzynka-bylego-pracownika-a-rodo/

Rekomendacja 4

Korzystając z bankowości elektronicznej, upewnij się, że jesteś na właściwej stronie

Rozwinięcie: korzystając z usług bankowych, upewnij się, że jesteś na właściwej stronie. Aby to sprawdzić, kliknij kłódkę w pasku adresu na górze przeglądarki i zobacz, dla kogo został wydany certyfikat bezpieczeństwa (tu powinna pojawić się właściwa strona banku – upewnij się, że w adresie nie ma literówek). Częstym sposobem na oszukanie odbiorcy za pomocą podmiany liter jest podmienianie małego „L" (jak Lucyna) czyli l z dużym „I" (jak Iwona) - prawda, że wyglądają identycznie? Zwróć na to uwagę!

Jeśli wyszukujesz stronę swojego banku w wyszukiwarce, nie wybieraj wyników będących reklamą (mogą się podszywać pod bank).

Linki do źródeł:

- https://www.bankier.pl/wiadomosc/CERT-wyludzaja-dane-przez-reklamy-Google-7968455.html
- https://zaufanatrzeciastrona.pl/post/szukasz-strony-banku-w-google-lepiej-dzisiaj-uwazaj/

Rekomendacja 5

Rozważnie publikuj treści na swój temat – chroń prywatność swoją i współpracowników

Rozwinięcie: dokładnie przemyśl co może znaleźć się w sieci na Twój temat, ostrożnie publikuj dane prywatne i dane osób z Tobą powiązanych. Pomyśl zanim podzielisz się prywatnym życiem z osobami w sieci. Stosuj zasadę im mniej, tym lepiej.

Jeśli komunikujesz działania organizacji, korzystaj z kanałów oficjalnych. Ustal, czy Twoi współpracownicy wyrażają zgodę na oznaczanie ich w postach lub na zdjęciach (jeśli nie, mogą też dokonać odpowiednich zmian w ustawieniach prywatności na danej platformie, np. Facebooku).

Nadmierne publikowanie faktów z Twojego życia jest niebezpieczne.

Linki do źródeł:

- https://trybawaryjny.pl/facebook-prywatnosc-poradnik/

Rekomendacja 6

Jeśli przygotowujesz i udostępniasz zrzuty ekranów, upewnij się, że zawierają tylko te informacje, które rzeczywiście chcesz przekazać

Rozwinięcie: jeśli na zrzucie ekranu znalazły się informacje, których nie chcesz udostępniać (np. inne karty przeglądarki lub Twoje dane osobiste), przytnij obraz lub zamaluj wybrane elementy w programie graficznym.

Podobną zasadę zastosuj w momencie udostępniania ekranu, np. podczas wideokonferencji.

> *Był to jeden z aspektów omawianych podczas szkolenia, niezwykle często pojawiający się element w trakcie codziennej pracy trenera czy prowadzącego spotkania*
>
> – Monika Pawlak, Fundacja Cooperacja

Linki do źródeł:

- https://www.screenpresso.com/

Rekomendacja 7

Jeśli masz problem z tworzeniem i zapamiętywaniem bezpiecznych haseł, korzystaj z menedżera haseł

Rozwinięcie: menedżer haseł to aplikacja, która generuje losowe i unikatowe hasła oraz przechowuje je w bezpieczny, szyfrowany sposób w pamięci komputera lub telefonu. Jest to niezbędne narzędzie do pracy organizacji. Korzystając z menedżera będziesz musiał(a) zapamiętać tylko jedno hasło (tzw. master password/hasło główne). Warto też zastosować podwójne uwierzytelnianie (np. potwierdzenie SMS-em lub mailem – w zależności od opcji konkretnej aplikacji), po to aby dodatkowo zwiększyć bezpieczeństwo menedżera.

Przykładowe narzędzia: LastPass lub 1password.

> *W projekcie dowiedziałem się o praktycznych zastosowaniach tego o narzędzia. Zainstalowałem sobie i wdrażam w życie codzienne*
>
> – Nick Bahur, Fundacja PCKK Edukacja i Rozwój

Linki do źródeł:

- https://sekurak.pl/menedzer-hasel-keepassxc-czy-jest-jak-uzywac-poradnik-od-sekuraka/
- https://pl.safetydetectives.com/best-password-managers/

Rekomendacja 8

Stwórz zbiór zasad określający „poziomy” dostępu do danych w Twojej organizacji

Rozwinięcie: dzięki temu dostęp do danego zbioru danych otrzymają wyłącznie te osoby, które będą z nich korzystać. W ten sposób ograniczysz ryzyko wycieku danych wrażliwych. Będzie Ci też łatwiej ustalić źródło ewentualnego wycieku.

Również dostęp do haseł/menedżera haseł powinien być ograniczony do niezbędnego minimum.

Rekomendacja 9

Komunikuj się ze swoimi współpracownikami za pośrednictwem bezpiecznych (szyfrowanych) komunikatorów

Rozwinięcie: warto zweryfikować, jakie komunikatory są wykorzystywane w organizacji dla przekazania informacji. Nie wszystkie są bezpieczne. Na chwile obecną jednym z najbardziej bezpiecznych jest aplikacja Signal. I nie posiada reklam :) Przykładowo, popularna w Polsce aplikacja Messenger nie jest szyfrowana; gromadzi informacje zarówno o treści wiadomości, jak i jej nadawcy/odbiorcy. I w związku z tym te informacje również mogą trafić w niepowołane ręce.

> *Na szkoleniu trenerzy dużo nam mówili o zagrożeniach związanych z wyciekiem danych. Teraz komunikuję się w bardziej bezpieczny sposób*
>
> – Hanna Shendzer, Fundacja „U-WORK"

Linki do źródeł:

- https://spidersweb.pl/2021/05/jaki-komunikator-wybrac-telegram-signal-viber-skype.html
- https://pl.vpnmentor.com/blog/najlepsze-bezpieczne-alternatywy-dla-whatsappa/

Rekomendacja 10

Zachowaj szczególną ostrożność, korzystając z usług bankowości elektronicznej

Rozwinięcie: nie działaj pod wpływem presji czasu, nawet jeśli otrzymujesz wiadomość/maila z ponagleniem o płatności. Sprawdzaj numery kont wpisywanych w przelewach. Upewnij się, czy numer jest właściwy, nawet jeśli go kopiujesz (zainfekowany komputer może umożliwić podmianę informacji przechowywanych w schowku). Zapoznaj się z definicjami różnych form oszustwa: phishing, whaling, smishing, vishing.

Linki do źródeł:

- https://www.totalmoney.pl/artykuly/376831,konta-osobiste,uwaga-na-wirusa-podmieniajacego-numery-kont-bankowych,1,1

Rekomendacja 11

Zapoznaj się uważnie z otrzymanym e-mailem lub SMS-em. Zanim klikniesz w link, zastanów się dwa razy, czy wiadomość pochodzi z bezpiecznego źródła

Rozwinięcie: bardzo ważne jest uważne czytanie maili i SMSów, które dostajemy. Takie przeoczone zagrożenie może kosztować utraty wszystkich danych.

Na co warto zwrócić uwagę:

- zachęta do natychmiastowego działania,
- błędy gramatyczne i w pisowni,
- wiadomość wydaje się wiarygodna, ale jeśli wczytać się uważniej, można zauważyć, że coś jest nie tak (np. zamiast słowa “faktura” jest słowo “kwitek”),
- masz wątpliwości, pokaż zaufanej osobie,
- www.mail.pl i www.mail-com.pl to są zupełnie różne strony internetowe,
- sprawdź opcję „Pokaż oryginał” w mailu, tam jest informacja o wysyłającym,
- najedź kursorem na link, aby upewnić się, że kryje się pod nim bezpieczna strona.

Dzięki wiedzy, którą dostałam na szkoleniu szybko udało mi się rozpoznać fałszywy mail i odpowiednio zareagować

– Hanna Shendzer Fundacja “U-WORK”

Linki do źródeł:

- https://www.gov.pl/web/baza-wiedzy/czym-jest-phishing-i-jak-nie-dac-sie-nabrac-na-podejrzane-widomosci-e-mail-oraz-sms-y
- https://pl.malwarebytes.com/phishing/
- https://kwestiabezpieczenstwa.pl/phishing/
- https://www.orange.pl/poradnik/twoj-internet/co-to-jest-phishing-i-jak-sie-przed-nim-bronic/

Rekomendacja 12

Minimalizuj ryzyko przejęcia konta poczty lub na portalach społecznościowych, korzystając z opcji uwierzytelniania dwuetapowego (dwuskładnikowego)

Rozwinięcie: uwierzytelnienie dwuetapowe jest prostym rozwiązaniem, które zwiększy bezpieczeństwo. Dzięki niemu zminimalizujesz ryzyko przejęcia konta mailowego, fanpage na Facebook czy Instagramie.

Istnieją różne formy podwójnego uwierzytelnienia. Najbezpieczniejszą jest korzystanie z fizycznego klucza (tzw. U2F), o którym więcej przeczytacie pod tym linkiem: https://niebezpiecznik.pl/post/klucze-u2f-pytania-i-odpowiedzi/.

Uwierzytelnianie dwuetapowe to podstawa bezpieczeństwa Twoich danych, nie traktuj go jako funkcje dla zaawansowanych. Jest absolutną koniecznością. Wraz z postępem technologicznym, to co 5 lat temu było umiejętnością zaawansowaną, dziś jest podstawą. Bądź na bieżąco

– Izabella Ferenc, Fundacja Rozwoju Społeczeństwa Informacyjnego

Linki do źródeł:

- https://www.gov.pl/web/baza-wiedzy/konfigurowanie-uwierzytelniania-dwuskladnikowego-2fa
- https://zaufanatrzeciastrona.pl/post/podstawy-bezpieczenstwa-uwierzytelnianie-dwuskladnikowe-po-co-i-jak-go-uzywac/
- https://pomoc.home.pl/baza-wiedzy/co-to-jest-uwierzytelnianie-dwuskladnikowe
- https://www.youtube.com/watch?v=Zr0PffkN09w&t=29s

Rekomendacja 13

Dbaj o bezpieczeństwo danych osobowych w e-korespondencji

Rozwinięcie: w sytuacji, gdy kierujesz maila do wielu osób, zadbaj o ich prywatność. W tym celu skorzystaj z opcji UDW/BCC, czyli „ukryte do wielu”. Jest to ważne również w kontekście RODO.

Linki do źródeł:

- https://support.google.com/mail/answer/2819488

Rekomendacja 14

Regularnie sprawdzaj, czy nie doszło do wycieku danych powiązanych z Twoim adresem e-mail

Rozwinięcie: wiedza o tym, jak identyfikować wycieki danych i reagować na nie jest bardzo ważnym elementem bezpieczeństwa w sieci. Warto regularnie zaglądać na stronę haveibeenpwnd.com, gdzie sprawdzisz, w jakich serwisach doszło do wycieku Twojego adresu e-mail (lub adresu organizacji).

Linki do źródeł:

- https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/
- https://pomoc.home.pl/baza-wiedzy/jak-sprawdzic-czy-moj-e-mail-wyciekl-do-sieci
- https://niebezpiecznik.pl/post/twoje-dane-wyciekly-a-my-znamy-darknety-czy-warto-placic-za-raporty-z-wyciekow/

Rekomendacja 15

Jeśli przekazujesz dane wrażliwe podczas rozmowy telefonicznej, poproś rozmówcę o podanie wcześniej ustalonego “słowa bezpieczeństwa”

Rozwinięcie: hasło bezpieczeństwa dla nadzwyczajnych sytuacji może uchronić od oszustwa. Sztuczna inteligencja rozwija się bardzo szybko i coraz częstsze są przypadki podróbki głosu.

Wyobraź sobie, że dzwoni do ciebie ktoś z rodziny bądź inna bliska osoba, z innego niż zwykle numeru telefonu (bądź nawet z tego, który masz zapisany), mówi, że ma duże problemy (np. została okradziona) i prosi o pilny przelew. Jeżeli wcześniej z tą osobą ustaliliście słowo bezpieczeństwa, to jest odpowiedni moment, żeby o nie zapytać. Wtedy będziesz pewien/pewna, że rozmawiasz z właściwą osobą, a nie z oszustem.

> *Wiedziałam o takim zagrożeniu przed szkoleniem, ale naiwnie myślałam, że mnie to nie dotyczy. Dowiedziawszy się o skali zagrożenia zrozumiałam, że będę czuła się bezpieczniej, jeżeli będę gotowa na ewentualną próbę oszustwa*
>
> – Hanna Shendzer Fundacja “U-WORK”

Linki do źródeł:

- https://br.atsit.in/pl/?p=87966

Rekomendacja 16

Nie przekazuj pochopnie numeru BLIK, którym dokonujesz przelewu lub płatności bezgotówkowej

Rozwinięcie: jeśli z jakichś przyczyn jest to konieczne, skontaktuj się z daną osobą telefonicznie*. Potwierdzisz w ten sposób tożsamość osoby, która zawiera transakcję. Możecie też ustalić wewnętrzne hasło, które należy podczas takiej rozmowy wypowiedzieć, aby rozwiać wszelkie wątpliwości.

*Technologia umożliwia w tej chwili również podszywanie się głosowe (choć nie jest to zjawisko powszechne, ze względu na koszty wykorzystania tej technologii). W związku z tym jeszcze bezpieczniejszą opcją będzie połączenie wideo.

Rekomendacja 17

Szyfruj przesyłane pliki (załączniki)

Rozwinięcie: szyfrowanie jest prostym rozwiązaniem, które znacznie zwiększa ochronę danych które przechowujesz i tych które przesyłasz. Zaszyfruj pliki, które przesyłasz, hasło do pliku prześlij inną drogą niż mailowe, np. sms. Jeśli przechowujesz dane na komputerze, szyfruj dyski.

Szyfrowanie zabezpiecza Twoje dane zarówno na Twojej poczcie, jak i na poczcie adresata (która może nie być tak dobrze zabezpieczona, jak Twoja :)).

Aby zaszyfrować plik z danymi wrażliwymi, np. umowę o pracę, sprawozdanie finansowe, skorzystaj z narzędzi takich jak 7ZIP lub WinRAR.

> *Nie wiesz, czy odbiorca należycie chroni swoją pocztę email. Zadbaj, by to, co przesyłasz, było bezpieczne również u odbiorcy. Szyfruj wysyłane pliki. Dzięki temu w razie wycieku danych z poczty odbiorcy pliki są bezpieczne. Pamiętaj, że to na nadawcy ciąży obowiązek właściwego zabezpieczenia przesyłanych dokumentów*
>
> – Izabella Ferenc, Fundacja Rozwoju Społeczeństwa Informacyjnego

Linki do źródeł:

- https://support.google.com/mail/answer/6330403?hl=pl
- https://portaldanych.pl/szybkie-szyfrowanie-zalacznikow-e-maili/

Rekomendacja 18

Zadbaj o to, aby dostęp do kamery i mikrofonu w Twoim urządzeniu był udzielany tylko zaufanym programom i tylko w określonych sytuacjach

Rozwinięcie: kamera i mikrofon w twoim urządzeniu mogą stanowić zagrożenie. Dobry program antywirusowy skanujący urządzenie na bieżąco jest najlepszą formą zabezpieczenia się przed nieuprawnionym wykorzystaniem mikrofonu/kamery przez podmioty nieuprawnione.

Linki do źródeł:

- https://support.google.com/chrome/answer/2693767
- https://support.microsoft.com/pl-pl/windows/windows-mikrofon-i-prywatno%C5%9B%C4%87-a83257bc-e990-d54a-d212-b5e41beba857
- https://support.mozilla.org/pl/kb/zarzadzanie-uprawnieniami-kamery-i-mikrofonu-firefox

Rekomendacja 19

Zabezpiecz hasłem telefon (i ważniejsze aplikacje)

Rozwinięcie: istnieje wiele sposobów zabezpieczenia telefonu hasłem i odblokowania: hasło (najlepiej skomplikowane), odcisk palca, rozpoznanie twarzy, znak graficzny. Spośród tych opcji najbezpieczniejszą/najskuteczniejszą jest hasło. Zarówno rozpoznanie twarzy jak i odcisk palca można skopiować, „podrobić".

Z pomocą programu antywirusowego lub ustawień wewnętrznych systemu (albo ustawień konkretnej aplikacji) zabezpiecz dostęp do wybranych aplikacji, np. bankowości mobilnej. Dzięki temu nawet jeśli Twój telefon jest odblokowany, osoby postronne nie będą mogły z nich korzystać.

Niezależnie skorzystaj z opcji szyfrowania urządzenia.

Linki do źródeł:

- https://www.tabletowo.pl/jak-ustawic-blokade-ekranu-zabezpieczyc-aplikacje-lub-swoje-pliki/
- https://antyweb.pl/blokada-ekranu-5-powodow-dla-ktorych-warto-miec-ja-wlaczona

Rekomendacja 20

Zabezpiecz się na wypadek kradzieży

Rozwinięcie: sprawdź, w jaki sposób możesz ustalić lokalizację swojego urządzenia, np. telefonu. Jeśli urządzenie nie ma włączonej lokalizacji (rekomendowane), sygnał pobliskich stacji pozwoli namierzyć Twój telefon.

Linki do źródeł:

- https://niebezpiecznik.pl/symantec/jak-zabezpieczyc-laptopa-kradzieza/
- https://support.google.com/accounts/answer/6160491?hl=pl

Rekomendacja 21

Pomyśl o założeniu maila „śmieciowego”

Rozwinięcie: oddziel pocztę organizacji/służbową od maili związanych z zakładaniem kont na portalach, w sklepach internetowych, itd. W ten sposób ograniczysz spam na oficjalnej skrzynce oraz ryzyko wycieku danych i dostępu do innych Twoich kont w przypadku takiego wycieku. Wykorzystaj tę skrzynkę w przypadku sporadycznego lub jednorazowego logowania się do usług internetowych.

Dla poprawy bezpieczeństwa nie łącz usług z kontem na Facebooku, ani z Twoim kontem Google.

Linki do źródeł:

- https://antyweb.pl/ile-adresow-e-mail

Rekomendacja 22

Nie korzystaj z logowania za pomocą konta Google lub na Facebooku

Rozwinięcie: jeśli utracisz dostęp do konta na Google lub Facebooku, możesz również stracić dostęp do innych usług/kont, z którymi te konta były powiązane. W przypadku wycieku hasła osoby postronne mogą uzyskać dostęp nie tylko do Twojego Facebooka czy konta Google, ale również do kont powiązanych.

Zamiast tego możesz skorzystać z menedżera haseł i wygenerować unikatowe hasło, które zostanie zapamiętane przez menedżer (Tobie pozostanie zapamiętanie hasła głównego).

Linki do źródeł:

- https://www.benchmark.pl/testy_i_recenzje/logowanie-przez-facebooka-czy-jest-bezpieczne.html
- https://antyweb.pl/logowanie-przez-facebooka

Rekomendacja 23

Przekaż wiedzę o bezpieczeństwie swoim współpracownikom

Rozwinięcie: bezpieczeństwo to proces: pamiętaj, aby regularnie odświeżać tę wiedzę. Ważne, aby o bezpieczeństwie w organizacji pamiętał cały zespół. Tylko stosowanie się do zasad przez wszystkie osoby pozwoli skutecznie ochronić Wasze dane.

Aktualizujcie wiedzę! Łańcuch jest tak mocny, jak mocne jest jego najsłabsze ogniwo. Zadbaj o to, by każde ogniwo (każdy pracownik) Twojej organizacji było maksymalnie świadome zagrożeń i posiadało aktualną wiedzę.

Rekomendacja 24

Zabezpiecz telefon programem antywirusowym i aktualizacją systemu

Rozwinięcie: pamiętaj o aktualizacji systemu i aplikacji, z których regularnie korzystasz. Możesz ustawić automatyczne aktualizacje, aby Twój sprzęt był zawsze maksymalnie chroniony (aktualizacje często zawierają poprawki błędów, które zwiększają bezpieczeństwo). Pobieraj programy antywirusowe wyłącznie ze stron producenta.

Dobre programy antywirusowe nie tylko chronią urządzenie i Twoje dane przed atakami, ale również pozwalają ukryć lokalizację (VPN), odszukać zagubione urządzenie, a nawet zdalnie zaszyfrować lub wykasować dane z urządzenia.

Linki do źródeł:

- https://support.microsoft.com/pl-pl/windows/aktualizacja-systemu-windows-3c5ae7fc-9fb6-9af1-1984-b5e0412c556a
- https://trybawaryjny.pl/musisz-aktualizowac-system/

Rekomendacja 25

Szyfruj dysk laptopa oraz dyski zewnętrzne

Rozwinięcie: pamiętaj o zaszyfrowaniu dysku komputera przenośnego, szczególnie jeśli korzystasz z niego w podróży lub w domu (poza miejscem pracy). Dodatkowo zaszyfruj wszystkie dyski zewnętrze, przede wszystkim te, na których przechowujesz kopie zapasowe. Dzięki temu osoby postronne nie będą miały wglądu w dane Twojej organizacji.

Linki do źródeł:

- https://kwestiabezpieczenstwa.pl/szyfrowanie-dysku/
- https://sekurak.pl/czym-jest-veracrypt-kompleksowy-poradnik-dotyczacy-szyfrowania-dyskow/

Rekomendacja 26

Zastanów się, czy na pewno potrzebujesz danej aplikacji

Rozwinięcie: z instalowaniem aplikacji wiążą się różne ryzyka, dlatego instaluj wyłącznie te, które są Tobie niezbędne. Nie eksperymentuj, jeśli nie masz pewności, jakie dane będą pobierane oraz kto i dla jakich celów je przetwarza. Sprawdź, jakie uprawnienia są niezbędne do poprawnego działania aplikacji i zastanów się, czy rzeczywiście chcesz je nadać. Bądź czujny/-a, jeśli aplikacja wymaga dostępu do aparatu, mikrofonu, galerii zdjęć, kontaktów lub innych wrażliwych danych.

Nie pobieraj pochopnie aplikacji, sprawdź uprawnienia aplikacji przed zainstalowaniem. Mimo że aplikacja jest w oficjalnym sklepie Play nadal może być aplikacją fałszywą, podszywającą się pod znane usługi, phishingową. Aplikacje bankowe pobieraj za pośrednictwem oficjalnej strony banku.

Linki do źródeł:

- https://trybawaryjny.pl/wiesz-pozwalasz-swoim-aplikacjom/
- https://support.google.com/googleplay/answer/6014972
- https://plblog.kaspersky.com/android-permissions-guide/6194/

Rekomendacja 27

Nie otwieraj załączników nieznanego pochodzenia lub z nieznanym rozszerzeniem

Rozwinięcie: taki załącznik może zawierać złośliwe oprogramowanie lub program instalujący się w tle pobierający dane z naszego urządzenia. Dobry program antywirusowy powinien rozpoznać zagrożenie, ale po co ryzykować :)

Linki do źródeł:

- https://bitdefender.pl/abc-cyberbezpieczenstwa-g-jak-grozne-wiadomosci-e-mail/
- https://www.instalki.pl/aktualnosci/bezpieczenstwo/42951-zlosliwe-zalaczniku-email-lista.html

Rekomendacja 28

Przyznawaj uprawnienia tylko niezbędnym plikom „cookies”

Rozwinięcie: nawet jeśli będziesz musiał(a) poświęcić na to trochę czasu - warto.

Linki do źródeł:

- https://support.google.com/accounts/answer/61416

Rekomendacja 29

Archiwizuj stare dane, usuwaj niepotrzebne

Rozwinięcie: archiwizuj dane, które nie są potrzebne w bieżącej pracy, ale które musicie lub chcecie zachować. Jednocześnie regularnie usuwajcie te pliki, które nie przydadzą się w przyszłości. Im mniej plików, tym mniejsze ryzyko, że wrażliwe dane trafią w niepowołane ręce.

Linki do źródeł:

- https://www.ebsco.com/e/pl-pl/blog/ronica-midzy-kopi-zapasow-a-archiwizacj-danych-i-dlaczego-ma-to-znaczenie

Rekomendacje dla NGO z zakresu:

TWÓRCZOŚĆ

Organizacja odpowiedzialna

INDID

4

Obszar:

Tworzenie dzieł/utworów/treści

Materiały tworzone w ramach działalności NGO w znacznej mierze powstają w celu służenia innym podmiotom jako źródło wiedzy lub inspiracji. Publikacje, broszurki, plakaty, prezentacje, grafiki, scenariusze – jeśli stworzyliście któreś z nich ramach działalności Waszej organizacji to brawa dla Was, bo stworzyliście dzieło. Zanim jednak je udostępnicie innym podmiotom (np. poprzez wrzucenie na stronę internetową) musicie podjąć szereg ważnych decyzji, o których często organizacje pozarządowe zapominają: w jaki sposób inne podmioty będą mogły korzystać z udostępnionych materiałów? Czy zgadzacie się aby np. zmieniano ich treść? Czy będzie można z nich korzystać w celach komercyjnych? Kwestie te nurtowały twórców (nie tylko z NGO-sów) od dawna, więc postanowiono opracować system licencji autorsko-prawnych, w których kompleksowo zawarte są odpowiedzi na wyżej postawione pytania. Od tego, na jaki zakres korzystania z dzieła stworzonego przez Waszą organizację przez inne podmioty się zgadacie, zależy to jaką licencję powinniście wybrać. Licencje autorsko-prawne, zwane powszechnie licencjami Creative Commons (CC) mogą składać się z czterech warunków:

1. Uznanie autorstwa (ang. Attribution, BY): zezwala się na kopiowanie, dystrybucję, wyświetlanie i użytkowanie dzieła i wszelkich jego pochodnych pod warunkiem umieszczenia informacji o twórcy. Uznanie autorstwa jest koniecznym elementem każdej licencji.
2. Użycie niekomercyjne (ang. Noncommercial, NC): zezwala się na kopiowanie, dystrybucję, wyświetlanie i użytkowanie dzieła i wszelkich jego pochodnych tylko w celach niekomercyjnych. Użycie dzieła w celach komercyjnych jest zatem niedozwolone.
3. Bez utworów zależnych (ang. No Derivative Works, ND): zezwala się na kopiowanie, dystrybucję, wyświetlanie tylko dokładnych (dosłownych) kopii dzieła, niedozwolone jest jego zmienianie.
4. Na tych samych warunkach (ang. Share Alike, SA): zezwala się na kopiowanie, dystrybucję, wyświetlanie i użytkowanie pochodnych dzieł, pod warunkiem, że będą one opublikowane na takiej samej licencji, czyli CC-SA.

Przykładowo jeśli stworzyliście raport z wynikami waszych obserwacji społecznych i zależy Wam aby go czytano i udostępniano, ale nie chcecie aby jego treść było zmieniana to powinniście użyć licencji CC-BY-ND. Aby w sposób prawidłowy oznaczyć utworzone dzieło wystarczy umieścić na nim oznaczenie licencji np. na początkowych stronach publikacji, w rogu grafiki. Pamiętaj, że mogą być bardzo różne rodzaje dzieł wykonanych w ramach działalności NGO. Dlatego najlepiej zapoznaj się z rodzajami licencji i wybierz odpowiednią https://creativecommons.pl/

Rekomendacja 1

Każde dzieło wytworzone w ramach działalności NGO powinno zostać oznaczone stosowną licencją autorsko-prawną

Rozwinięcie: zapoznaj się z rodzajami licencji i wybierz odpowiednią https://creativecommons.pl/

Rekomendacja 2

Autorem/autorami dzieł wytworzonych przez NGO (w znaczeniu osobistych praw autorskich) nigdy nie jest samo NGO, a konkretna osoba/osoby fizyczne, dlatego należy je opatrzyć nazwiskiem/ami osób jako twórców (autorów) dzieła

Rekomendacja 3

NGO może dysponować jedynie majątkowymi prawami autorskimi do dzieła wytworzonego w ramach swojej działalności, dlatego powinno zadbać o odpowiednią umowę przekazania autorskich praw majątkowych przez autora (posiadającego osobiste prawa autorskie)

Rozwinięcie: umowy zawierane między NGO a wykonawcą/ami dzieła powinny być maksymalnie precyzyjne w zakresie przenoszenia autorskich praw majątkowych. Osobiste prawa autorskie, to coś innego niż majątkowe prawa autorskie! Te pierwsze na zawsze należą do twórcy (konkretnej osoby), natomiast te drugie mogą być zmieniane.

Rekomendacja 4

Informacja o źródle finansowania danego dzieła nie jest wystarczająca w kwestiach związanych z prawami autorskimi - NGO musi oznaczyć także autora/ów oraz ewentualne możliwości wtórnego wykorzystania (stosowne oznaczenie licencji autorsko-prawnej)

Rekomendacja 5

Jeśli NGO tworzące dzieła (np. publikacje) chce aby były one później wykorzystywane w innych dziełach powinno oznaczać je licencją CC BY-SA (uznanie autorstwa - na tych samych warunkach)

Rekomendacja 6

Jeśli NGO tworzące dzieła (np. publikacje) nie chce aby były one później wykorzystywane w innych dziełach powinno oznaczać je licencją CC BY-ND (uznanie autorstwa - bez utworów zależnych)

Rekomendacja 7

Jeśli NGO nie chce aby dzieło powstałe w wyniku ich prac było wykorzystywane komercyjnie powinno dodatkowo do opisu licencji dołączyć oznaczenie: -NC (użycie niekomercyjne)

Rekomendacja 8

Własne wytwory NGO udostępniane na zasadzie licencji Open Source warto umieszczać w bazach wolnego dostępu

Link: jednym z ciekawszych jest https://ngoteka.pl/

Rekomendacja 9

NGO zawierając umowę z wykonawcą dzieła powinno w pierwszej kolejności zadbać o własne interesy w kwestii majątkowych praw autorskich

Komentarz: jeżeli twórca dzieła (osoba prywatna) ma nieczyste intencje, to źle skonstruowana umowa z tą osobą może dać jej ogromne możliwości utrudniania korzystania z dzieła przez organizację. Taka sytuacja może mieć także miejsce w przypadku, kiedy NGO rozstaje się w konflikcie z kimś, kto tworzył dla niego dzieła (to się niestety zdarza).

Rekomendacja 10

Podpisując umowę na realizację projektu z grantodawcą (publicznym bądź prywatnym) NGO powinno zadbać o sposób wykorzystywania dzieł wytworzonych podczas projektu w zakresie autorskich praw majątkowych

Rekomendacja 11

NGO nie powinno godzić się na przekazywanie całości autorskich praw majątkowych podmiotom trzecim (np. jednostkom samorządu terytorialnego, na zlecenie których realizują dane działanie, bądź firmom)

Rozwinięcie: czasem warunkiem podpisania umowy ze strony JST, bądź firmy prywatnej jest przekazanie autorskich praw majątkowych tej jednostce przez NGO. Wynika to czasem z jednolitych wzorów umów, które funkcjonują w urzędach od lat.

Kiedyś firma warunkowała współpracę z nami od tego czy przekażemy całość praw majątkowych do wykonanych dzieł. To niedopuszczalne

- Adam Siger, Fundacja Udaru Mózgu

Rekomendacja 12

NGO powinno zwracać uwagę na kwestię praw autorskich także kiedy chce realizować projekty unijne i we współpracy z innymi podmiotami

Rozwinięcie: nie ma sytuacji, projektów, w których NGO by było zwolnione z zadbania o tę kwestię.

Obszar:

Korzystanie z treści/dzieł

Rekomendacja 13

Pozyskując jakieś dzieło (np. kupując/pobierając publikację od innego podmiotu) NGO, co do zasady, nie zyskuje autorskich praw majątkowych do niego, a jedynie możliwość wykorzystania na użytek własny, zgodnie z licencją, jaka została przypisana do dzieła

Rekomendacja 14

W działalności NGO warto korzystać z zasobów typu OpenSource (np. Pixabay, Unsplash, wyszukiwarki Creative Commons, Wikipedia, Wikimedia)

Linki do źródeł:

- pixabay.com
- otwartezasoby.pl
- https://thenounproject.com/browse/icons/recent/?p=1

Rekomendacja 15

NGO nie powinno korzystać z grafik/zdjęć/itp. znalezionych w wyszukiwarkach (np. w Google), których licencja nie została wyraźnie oznaczona. Podanie w opisie źródła grafiki/zdjęcia linka do niego nie jest wystarczające w kwestiach związanych z prawami autorskimi

Komentarz: jeśli chcemy korzystać z grafik/zdjęć/itp. znalezionych w wyszukiwarkach musimy upewnić się, że posiadają jasno określoną licencję. Jeżeli licencja nie została określona - potrzebujesz zgody autora, a o to zazwyczaj bardzo trudno.

Możesz korzystać z darmowych banków zdjęć i grafik np.:

- pixabay.com
- otwartezasoby.pl
- https://thenounproject.com/browse/icons/recent/?p=1

Rekomendacja 16

Kwestia praw autorskich powinna być tez uwzględniana jeśli organizacja sprzedaje prace swoich uczestników/podopiecznych na kiermaszach

Komentarz: należy podpisać umowę z uczestnikami/wolontariuszami organizacji lub ich przedstawicielami ustawowymi (rodzicami/opiekunami), która umożliwia przenosi autorskie prawa majątkowe na organizację. W takiej sytuacji sprzedaż tych prac będzie zgodna z prawem.

Rekomendacja 17

Czytaj regulaminy stron, z których pobierasz treści - one się potrafią co jakiś czas zmieniać!

Obszar:

Promocja działań NGO

Rekomendacja 18

Organizacja powinna dysponować własnym logotypem, który zostanie przygotowany w kilku wariantach

Komentarz: różne warianty, to przede wszystkim wersja podstawowa logo (najlepiej mieszcząca się w granicach kwadratu), a także rozszerzona, która będzie mogła być umieszczona na szerszych materiałach. Chodzi także o różne wersje kolorystyczne, szare oraz na przezroczu.

Rekomendacja 19

Logotyp NGO powinien być dostępny dla zespołu także w formie grafiki wektorowej, aby zapewnić jego wysoką jakość w różnych publikacjach i gadżetach

Rekomendacja 20

NGO powinno zadbać o stworzenie spójnej strategii promocyjnej (obok innych strategii, np. organizacyjnej czy fundraisingowej), która obejmować będzie horyzont co najmniej 2-3 lat

Rozwinięcie: Strategia promocyjna powinna być weryfikowana co najmniej raz w roku. Powinna ona być dokumentem praktycznym, który realnie wpływa na działania, a nie samym „dokumentem dla dokumentu”.

Rekomendacja 21

Wyznacz jedną osobę w ramach działań promocyjnych NGO w sieci odpowiedzialną za całokształt promocji

Rekomendacja 22

W ramach działań promocyjnych NGO powinno dysponować ujednoliconą identyfikacją wizualną (spójne logotypy + fonty)

Rekomendacja 23

NGO powinno dysponować księgą znaku w zakresie własnej identyfikacji wizualnej, która będzie prezentować i regulować sposoby wykorzystania elementów graficznych logo organizacji

Rekomendacja 24

W przypadku braku możliwości finansowych bądź organizacyjnych w zakresie tworzenia własnej oprawy graficznej NGO może spróbować pozyskać młodych grafików za darmo na zasadzie współpracy „do portfolio" lub od jakiejś firmy, która oferuje takie usługi w ramach CSR

Rozwinięcie: Pamiętajcie, że z każdą z firm, z którą współpracujemy na zasadzie CSR musimy podpisać umowę w zakresie współpracy i przekazania praw autorskich. Mogą być ukryte koszty. Nawet w przypadku współpracy darmowej z grafikiem należy zadbać o odpowiednią umowę i przeniesienie autorskich praw majątkowych do stworzonych elementów graficznych

Rekomendacja 25

Przydatnym narzędziem do tworzenia grafik w NGO jest online'owy program CANVA, którego wersja PRO jest dostępna za darmo dla organizacji pozarządowych

Link do źródeł: canva.com

Rekomendacja 26

Własny logotyp/własne logotypy NGO może zastrzec jako znak towarowy w urzędzie patentowym, aby uchronić się przed jego/ich niepożądanym wykorzystaniem przez inne podmioty

Rekomendacja 27

NGO powinien aktywnie działać w mediach społecznościowych dostosowując przekaz do specyfiki danego medium - inaczej formułować komunikaty na FB, Twitterze czy Instagramie

Rekomendacja 28

Działania promocyjne NGO w mediach społecznościowych muszą być etyczne

Rekomendacja 29

NGO - w miarę możliwości - nie powinno uzależniać się od jednego medium w zakresie komunikowania się z odbiorcami (np. od Facebooka). Warto inwestować we własną stronę internetową i na niej budować infrastrukturę angażującą

Rekomendacja 30

Organizacja powinna rozważyć czy chce dokonywać płatnej promocji na kanałach społecznościowych wielkich koncernów (typu FB, Youtube, Twitter, itp.) Jeśli tak, to płatne kampanie powinny być precyzyjnie sprofilowane pod odpowiednie grupy odbiorców

Rekomendacja 31

Szczególną formą promocji działań NGO jest Google Ads (wcześniej Google AdWords), która umożliwia pozycjonowanie strony organizacji w wyszukiwarce Google po wpisaniu odpowiednich słów kluczowych.

Rekomendacja 32

Rekomendacja nawiązania współpracy z dużymi koncernami, które mają dedykowane programy dla NGO np. Microsoft Office, TechSoup

ISBN 978-83-952071-8-1

Publikacja powstała w ramach projektu *Szkoła Odpowiedzialności Cyfrowej NGO* realizowanego dzięki dotacji otrzymanej z programu Aktywni Obywatele – Fundusz Krajowy finansowanego z Mechanizmu Finansowego Europejskiego Obszaru Gospodarczego

Iceland
Liechtenstein
Norway
Active citizens fund

INDID
Instytut Dyskursu
i Dialogu

DEMAGOG

SOCNGO
Szkoła Odpowiedzialności Cyfrowej