Rekomendacje dla organizacji pozarządowych

w zakresie odpowiedzialnych działań w sieci

SOCNGO
Szkoła OdpowiedzialnościCyfrowej

Rekomendacje zostały wypracowane w ramach projektu
Szkoła Odpowiedzialności Cyfrowej NGO

EDYCJA III

przeznaczona dla organizacji rzeczniczych

Moduł RZETELNOŚĆ

Monika Bartlińska, Iwona Kozieja,
Piotr Rączkowiak

Mentor: Sara Smyczek-Gołębiewska (INDID)

Moduł BEZPIECZEŃSTWO

Aleksandra Jurasz, Ewa Rembikowska,
Sylwia Ryń, Martyna Szypuła, Błażej Zając

Mentor: Aleksy Szymkiewicz (Demagog)

Moduł PRAWDA

Ziemowit Dziopa, Teresa Niewiadomska,
Violetta Stokfisz, Martyna Szypuła,
Izabela Warska-Tymowicz, Justyna Żyndul

Mentor: Aleksy Szymkiewicz (Demagog)

Moduł TWÓRCZOŚĆ

Iza Jania, Aleksandra Jurasz, Kosma Kołodziej,
Teresa Niewiadomska, Ewa Rembikowska,
Piotr Rączkowiak, Violetta Stokfisz

Mentor: Sara Smyczek-Gołębiewska (INDID)

Korekta

Monika Tańska

Opracowanie graficzne

Sara Pszonka

INDID
Instytut Dyskursu i Dialogu

DEMAGOG

Iceland Liechtenstein Norway Active citizens fund

Wstęp

Prezentujemy Państwu trzecią publikację wypracowaną wspólnie przez Uczestników i Uczestniczki projektu „Szkoła Odpowiedzialności Cyfrowej NGO". Jest to publikacja niezwykle ważna, ponieważ zbiera rekomendacje dla organizacji pozarządowych w zakresie **odpowiedzialnych działań w sieci.** Tym razem dedykowana jest ona organizacjom prowadzącym działalność rzeczniczą, czyli próbującym dokonywać instytucjonalno-prawnych zmian na rzecz różnych grup społecznych lub w imię istotnych dla nich wartości. Głęboko wierzymy, że wskazówki i sugestie w niej zawarte posłużą do wprowadzenia zdrowych nawyków wśród przedstawicieli/ek różnych NGO-sów, co sprawi, że funkcjonowanie tych podmiotów będzie **oparte na prawdzie, rzetelniejsze, bezpieczniejsze i bardziej twórcze.** Podobnie jak w przypadku poprzednich publikacji nawiązujemy tu do nazw modułów funkcjonujących w ramach projektu, wspólnie łączących się w słowie **ODPOWIEDZIALNOŚĆ**, które stało się motywem przewodnim tego przedsięwzięcia. Współcześnie żyjemy w erze skokowego rozwoju cyfrowo-technologicznego. Dzięki niemu organizacje pozarządowe zyskały niewyobrażalne możliwości, ale także stają przed zagrożeniami, jakich do tej pory nie było. Właśnie dlatego postanowiliśmy w ramach projektu (my, czyli Instytut Dyskursu i Dialogu oraz Stowarzyszenie Demagog) zwrócić uwagę zarówno na te pierwsze, jak i te drugie oraz wyposażyć NGO-sy w narzędzia umożliwiające **mądre – czyli odpowiedzialne – działania w sieci.**

Tysiące 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. NGO-sy powinny być w pełni świadome tych niebezpieczeństw i powinny wprowadzać do swoich działań **mechanizmy** przed nimi **chroniące.**

Nierzadko fundacje czy stowarzyszenia podczas realizowania swoich projektów dysponują środkami publicznymi lub pozyskanymi z grantów/darowizn od podmiotów prywatnych lub darczyńców. Utrata ich wskutek wyłudzenia w sieci mogłaby skutkować ogromnymi problemami dla samej organizacji czy członków zarządu, nie mówiąc o stratach wizerunkowych. Podstawową rolą NGO jest **zabezpieczyć środki finansowe** i sprawić, aby realizacja celów statutowych odbywała się **w pełnej zgodności z prawem**, także w często niedocenianej sferze działań cyfrowych. Marzy nam się, aby dzięki projektowi „Szkoła Odpowiedzialności Cyfrowej NGO" oraz wypracowanym w jego ramach publikacjom, NGO-sy stały się przykładem do naśladowania w zakresie odpowiedzialnych działań w sieci. Szczególną rolę odgrywają organizacje o charakterze rzeczniczym. Tworzą je najczęściej ludzie o otwartych głowach pełnych pomysłów, którzy czasami przedkładają realizację misji nad bezpieczeństwo cyfrowe. W dobie komunikacyjnego prymatu mediów społecznościowych nie zawsze jest to postawa odpowiedzialna. Liczymy, że ta publikacja nie będzie jedynie teoretyczną pozycją na długiej liście „do przeczytania", ale że jak najszybciej wpłynie na **realne, PRAKTYCZNE działania i procedury** w trzecim sektorze, zwłaszcza wśród organizacji rzeczniczych. Stworzenie ostatecznego kształtu rekomendacji zawartych w niniejszej publikacji wymagało wiele pracy i zaangażowania od Uczestników i Uczestniczek drugiej 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. Ich nazwiska znaleźć można wśród autorów niniejszej publikacji. Tym razem za opracowanie graficzne i wydanie publikacji odpowiadał Partner projektu – Stowarzyszenie Demagog, któremu niniejszym bardzo serdecznie dziękuję za zaangażowanie i profesjonalizm w działaniach. Publikacja 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"

01 Rzetelność

02 Prawda

03 Bezpieczeństwo

04 Twórczość

INDID
Instytut Dyskursu
i Dialogu

Stosuj tzw. double check (podwójne sprawdzenie) 01

Rozwinięcie

Gdy pracuje się pod presją czasu, zdarza się popełniać błędy. Dobrze jest mieć w zespole osoby, które zweryfikują napisaną treść pod kątem prawidłowości danych. Pozwoli to uniknąć wprowadzania poprawek do tekstu po jego publikacji. Warto też poprosić drugą osobę o sprawdzenie treści pod kątem poprawności językowej (literówki, błędy ortograficzne czy stylistyczne).

Zanim opublikujesz – zastanów się i oceń rzetelność 02

Rozwinięcie

Stwórz sobie skalę rzetelności, np. od 1-10, i oceń rzetelność informacji. Ustal też poziom rzetelności, który muszą spełniać wszystkie Twoje publikacje. W niektórych sytuacjach warto zaangażować drugą osobę do oceny rzetelności.

Nie publikuj, jeśli masz wątpliwości 03

Rozwinięcie

Jeżeli nie masz pewności, że informacja jest rzetelna, może warto zrezygnować z publikacji. Zrobisz to, gdy będziesz mieć więcej czasu na jej przygotowanie i sprawdzenie źródeł. Czasem chęć publikacji jest tak duża, że może odbyć się kosztem jakości i rzetelności tekstu.

Korzystaj z wiedzy ekspertów 04

Rozwinięcie

Przy tematach trudnych lub rozbudowanych warto wspierać się ekspertami zewnętrznymi. Jeśli posiadasz środki finansowe i czasowe, zaangażuj fachowców, ponieważ nie zawsze to, co nam się wydaje, jest faktycznie wiedzą ekspercką.

Zadbaj, aby treści były spójne 05

Rozwinięcie

Określ styl komunikacyjny organizacji. Uwzględnij przy tym m.in.: grupę odbiorców, główny przekaz, profil organizacji. Spójność publikacji pomoże zbudować silną bazę czytelników oraz zwiększyć ich zaufanie do organizacji.

Pamiętaj, aby dostosować treści do osób z niepełnosprawnościami 06

Rozwinięcie

Warto poświęcić trochę czasu i zapoznać się z tworzeniem dostępnych treści. Jest wiele bezpłatnych źródeł na ten temat, np. → *gov.pl*

Zawsze wskazuj źródła informacji 07

Rozwinięcie

Gdy podajesz informację, jej źródło umieść w tekście lub skorzystaj z przypisu źródłowego. W ramach dłuższego tekstu (np. na stronie lub na blogu) warto wskazać bibliografię (wraz z linkami). Zwiększy to wiarygodność publikacji oraz umożliwi czytelnikom zweryfikowanie stawianych przez Ciebie tez.

Przygotuj treści z odpowiednim wyprzedzeniem czasowym 08

Rozwinięcie

Jeśli masz bardzo mało czasu, może warto odpuścić publikowanie newsa na rzecz dobrze przygotowanej fotorelacji z komentarzem lub obszernego raportu podsumowującego. Dobry plan to połowa sukcesu!

Miej na uwadze różnorodność podmiotów prowadzących badania 09

Rozwinięcie

Weryfikuj swoich zleceniobiorców. Czasem wystarczy sprawdzić w internecie, kto zaufał danej firmie, i poprosić o opinię (np. telefoniczną). Sprawdzaj wcześniejszą działalność oraz zespół badawczy podmiotów, które stoją za wykonaniem konkretnych badań, a także ich finansowanie oraz metodologię pracy.

Gdy z różnych względów nie możesz opublikować całości przekazu, wstaw link do rozszerzonej wersji 10

Rozwinięcie

Odbiorcy w mediach społecznościowych chętniej czytają proste i krótkie komunikaty. Jednak część osób może oczekiwać rozwinięcia tematu i poznania szczegółów. Ponadto – aby uniknąć przytaczania zdań wyrwanych z kontekstu – warto dołączyć link do rozbudowanej wersji komunikatu (np. link do strony z publikacją).

01 Rzetelność

02 Prawda

03 Bezpieczeństwo

04 Twórczość

DEMAGOG

W przypadku, gdy Twoją organizację dotknie kampania dezinformacyjna, sprawdź źródła tej kampanii

01

Rozwinięcie

Sprawdź:

- kto jest jej autorem
- na co się powołuje
- jakich argumentów używa
- doszukaj się celu lub powodu tej kampanii
- gdzie jest ona umieszczona
- sprawdź swoje powiązania z autorem

Przygotuj dla swojej organizacji procedury reagowania na dezinformację

02

Rozwinięcie

Procedury:

- sprawdź źródło, autora, przeanalizuj treść i cel
- przygotuj oświadczenie
- zadbaj o przejrzystość
- poinformuj zespół
- powołaj zespół ekspercki
- przedyskutuj w swoim zespole
- znajdź najlepszy sposób reagowania

Komentarz

Warto mieć przygotowane procedury, ponieważ – gdy uderzy w nas kampania dezinformacyjna – szkoda czasu na opracowywanie sposobów działania. Taki plan przyśpieszy reakcję. // Martyna Szypyła, Stowarzyszenie Inicjatyw Społecznych Nasz Dom

Nie lekceważ nawet nieznacznych aktywności, przejawów działań dezinformacji. Pamiętaj, że to zawsze może uderzyć w twoje działania i wizerunek. // Teresa Niewiadomska, Stowarzyszenie Rodzin Katolickich

Pamiętaj o źródłach 03

Rozwinięcie

Zadbaj o podawanie źródeł, gdy zamieszczasz swoje posty, relacje czy teksty. Gdy zamieszczasz źródła, pamiętaj o autorach zdjęć, dokumentów, relacji, materiałów. Zadbaj, by źródła finansowania zarówno twoje, jak i pozostałych organizacji, o których mówisz, były przejrzyste. Pamiętaj o pełnych nazwach projektów i realizowanych działań.

Znajdź eksperta 04

Rozwinięcie

Warto wyznaczyć co najmniej jedną osobę jako eksperta ds. weryfikacji informacji. Może ona zajmować się wyłącznie ich weryfikacją, sprawdzać źródła i szukać manipulacji.

Masz prawo odmówić współpracy 05

Rozwinięcie

Jeśli jakaś organizacja nie podziela wartości Twojej organizacji, to pamiętaj, że możesz odmówić współpracy.

Komentarz

Jeśli chcesz nawiązać współpracę, to pamiętaj, żeby obserwować działania innej organizacji przez dłuższy czas. Zwracaj uwagę na posty, komentarze, treści - sprawdzaj całokształt. Na pierwszy rzut oka jakieś NGO może wydawać się obiektywne i apolityczne, jednak po dłuższej obserwacji możemy zauważyć inny kontekst działania. // Violetta Stokfisz, Koło Gospodyń Wiejskich w Dąbrowie

Stwórz bazę narzędzi do weryfikacji informacji 06

Rozwinięcie

Warto stworzyć bazę narzędzi, które pozwolą na szybkie i poprawne weryfikowanie informacji.

Przykładowe narzędzia:

- *archive.org*
- *whois.domaintools.com*
- *whopostedwhat.com*
- *exiftool.org*

Stwórz bazę zaufanych kontaktów i organizacji 07

Rozwinięcie

Warto stworzyć bazę zaufanych kontaktów i organizacji, które są przykładem do naśladowania i dobrymi współpracownikami we wspólnych projektach.

Zadbaj o transparentność działań organizacji 08

Rozwinięcie

Ważna jest transparentność organizacji. Wszystkie działania muszą być przejrzyste, sensowne, poparte konkretnymi celami, które organizacja chce osiągnąć. Warto również prowadzić otwartą komunikację i dokumentację.

Komentarz

Im bardziej będziemy dbać o transparentny wizerunek, tym mniej będziemy stresować się podczas możliwych oskarżeniach. // Teresa Niewiadomska, Stowarzyszenie Rodzin Katolickich

Dbaj o przejrzystość działań i finansów, ponieważ darczyńcy śledzą naszą aktywność i chcą być pewni działań. // Violetta Stokfisz, Koło Gospodyń Wiejskich w Dąbrowie

Nie działaj pod wpływem emocji 09

Rozwinięcie

W działaniach i podczas weryfikowania informacji kieruj się faktami, a nie – emocjami. Dezinformacja bazuje na emocjach, dlatego ludzie bardzo łatwo w nią wierzą.

Komentarz

Każde działanie i każdą wypowiedź warto przemyśleć. Działanie pod wpływem emocji często jest zgubne i może prowadzić do zaostrzenia czy to konfliktu, czy – kampanii dezinformacyjnej. // Martyna Szypyła, Stowarzyszenie Inicjatyw Społecznych Nas Dom

Korzystaj z wielu źródeł informacji 10

Rozwinięcie

Weryfikuj informacje na podstawie wielu źródeł, aby uzyskać najbardziej wiarygodny pogląd na sytuację.

Komentarz

Bazowanie na jednym źródle może być zgubne. Organizację tworzą ludzie, a ludzie popełniają błędy, więc warto bazować na wielu źródłach. // Ziemowit Dziopa, Młodzi dla Torunia

Zadbaj o edukację członków organizacji 11

Rozwinięcie

W celu obrony przed dezinformacją i kampaniami uderzającymi w wiarygodność naszej organizacji, warto zadbać o wyedukowanie członków organizacji, tak by ci poznali techniki manipulacji i sposoby na ochronę przed nimi.

Komentarz

Ciągła troska o współpracowników to praktyka, która pozwala na utrzymanie relacji z dobrymi pracownikami. Dzięki temu podnosisz standardy ich działań i kompetencje. // Teresa Niewiadomska, Stowarzyszenie Rodzin Katolickich

Wspólne szkolenia prowadzą również do większej spójności działań. Wspólne szkolenia, np. z bezpieczeństwa, pozwalają zadbać o całokształt organizacji i faktycznie wdrożyć je jako wspólną praktykę. // Violetta Stokfisz, Koło Gospodyń Wiejskich w Dąbrowie

01 Rzetelność

02 Prawda

03 Bezpieczeństwo

04 Twórczość

DEMAGOG

Używaj długich i unikatowych haseł 01

Rozwinięcie

Hasło powinno zawierać minimum 18 znaków w ciągu przypominającym zdanie, wers rymowanki lub wiersza. Pamiętaj o używaniu dużych i małych liter, cyfr oraz symboli. Im dłuższe hasło, tym trudniej je złamać. Używaj różnych haseł dla różnych platform. Nie przekazuj haseł osobom postronnym. Zadbaj o to, aby w organizacji były co najmniej dwie zaufane osoby mające dostęp do bazy haseł.

Komentarz

Testowałam kiedyś program do łamania haseł. Czas poświęcony na łamanie tradycyjnego 8-znakowego hasła (duża litera, mała litera, cyfra, znak specjalny) – minuta. // Martyna Szypuła, Stowarzyszenie Inicjatyw Społecznych Nasz Dom

Używaj menadżera haseł oraz długich, bezpiecznych haseł 02

Rozwinięcie

Jeśli masz problem z zapamiętywaniem haseł – skorzystaj z menadżera haseł Google lub ze specjalnych programów, takich jak Bitwarden czy NordPass. Każdy menadżer haseł będzie lepszym rozwiązaniem niż jedno hasło do wielu platform.

Używaj szyfrowanych komunikatorów 03

Rozwinięcie

Korzystaj z bezpiecznych komunikatorów, które stosują szyfrowanie E2E, czyli End To End – tylko osoby kontaktujące się mogą zobaczyć wiadomość: wysyłający szyfruje, odczytujący rozszyfrowuje. Polecane komunikatory to: Signal, Whatsapp, Telegram. Program obsługujący skrzynki pocztowe: Thunderbird.

Komentarz

Warto znaleźć taki komunikator, który nigdy w swojej historii nie miał wycieku danych oraz wykorzystuje technikę E2E, która skutecznie uniemożliwia śledzenie naszych rozmów przez osoby trzecie. // Martyna Szypuła, Stowarzyszenie Inicjatyw Społecznych Nasz Dom

Dbaj o szyfrowanie danych (dyski, skrzynki pocztowe) 04

Rozwinięcie

Pamiętaj, że ważne dokumenty dotyczące projektów lub kwestii finansowych, a także dane wrażliwe pracowników czy beneficjentów, powinny być dobrze zabezpieczone i zaszyfrowane na lokalnych lub sieciowych dyskach. Pamiętaj, że jeśli wysyłasz e-maile grupowe, musisz ukryć dane pozostałych odbiorców.

Dbaj o aktualizacje oprogramowania i pobierz program antywirusowy na wszystkie urządzenia 05

Rozwinięcie

Aktualne oprogramowanie i program antywirusowy mogą Cię uratować przed złośliwym oprogramowaniem, przesyłanym chociażby w e-mailach. Aktualizacje oprogramowania należy wdrażać na wszystkich urządzeniach, z których korzystasz.

Wielokrotnie weryfikuj nadawców e-maili 06

Rozwinięcie

- Sprawdzaj błędy ortograficzne, literówki, stylistykę.
- Zweryfikuj, czy adres mailowy jest powiązany z firmą lub z organizacją (sprawdź, czy adres jest powiązany z domeną).
- Nie klikaj w linki z maili lub sprawdź je w browserlingu (http://browserling/com).

Warto zwrócić uwagę, w jakim stylu napisano wiadomość. Ataki phishingowe często opierają się na emocjach, takich jak strach, lęk czy radość (coś wygrałeś lub coś tracisz). Dzięki reakcjom emocjonalnym stają się dla nas bardziej wiarygodne (na pierwszy rzut oka).

Komentarz

E-maile od oszustów są łudząco podobne do e-maili pochodzących z prawdziwych źródeł. Dlatego warto zachować czujność i weryfikować każdy otrzymany e-mail, ponieważ jednym kliknięciem możesz pobrać złośliwe oprogramowanie na swój komputer i podać oszustowi swoje wrażliwe dane. // Martyna Szypuła, Stowarzyszenie Inicjatyw Społecznych Nasz Dom

Przygotowanie procedur kryzysowych 07

Rozwinięcie

Wyznacz odpowiednie osoby do poszczególnych działań. Opracuj schemat reakcji na różne ewentualności, takie jak:

- włamanie na pocztę
- kradzież danych
- utrata danych
- ściągnięcie złośliwego oprogramowania.

Komentarz

Miałam kiedyś sytuację, gdy siostra dostała wiadomość SMS z PGE i kliknęła w link przekierowujący do płatności. Przestraszyła się i była pewna, że włamano się jej na konto. Na szczęście samo kliknięcie w link nie zawsze skutkuje utratą dostępów lub środków. // Sylwia Ryń, Fundacja Sarigato

Dbaj o tworzenie kopii zapasowej 08

Rozwinięcie

Pamiętaj o regularnym tworzeniu backupów. Możesz do tego wykorzystać dysk przenośny lub chmurę. Zawsze można w ten sposób odzyskać dane, które są odpowiednio zabezpieczone.

Wyznacz osobę, która będzie odpowiadała za bezpieczeństwo Twojej organizacji 09

Rozwinięcie

Wyznaczenie osoby, która będzie zajmowała się technicznymi aspektami bezpieczeństwa organizacji. Do jej zadań powinno należeć:

- aktualizacja oprogramowania na urządzeniach organizacji
- bezpieczne przechowywanie wszystkich haseł
- cykliczny audyt bezpieczeństwa ze skupieniem się na lukach bezpieczeństwa
- tworzenie kopii zapasowych
- szyfrowanie dysków, e-maili.

Komentarz

Warto szkolić pracowników i uświadamiać ich w kwestii bezpieczeństwa, ale dobrze, żeby jeden pracownik był ekspertem w tej dziedzinie i dbał o całokształt bezpieczeństwa organizacji. // Martyna Szypuła, Stowarzyszenie Inicjatyw Społecznych Nasz Dom

Zakrywaj kamerkę w komputerze, jeśli jej nie używasz 10

Rozwinięcie

Istnieją specjalne osłony na kamerkę. Wypracuj nawyk zasłaniania kamery zawsze, gdy jej nie używasz.

Pamiętaj o standardowych krokach bezpieczeństwa, gdy zgubisz lub utracisz telefon 11

Rozwinięcie

- Skontaktuj się z twoim operatorem sieci i spytaj, czy ktoś prosił o udostępnienie duplikatu karty.
- Zablokuj kartę SIM.
- Zmień hasła do wszystkich kont (aplikacje banków, portale społecznościowe, komunikatory).
- Zgłoś kradzież telefonu na policję (warto znać numer IMEI).

Higiena i cyfrowe nawyki w NGO 12

Rozwinięcie

Co możesz zrobić, aby poprawić swój dobrostan cyfrowy, a tym samym – zwiększyć bezpieczeństwo swojej organizacji?

Staraj się utrzymywać harmonię pomiędzy życiem offline a życiem online. Nawet jeśli pracujesz zdalnie, wyznacz sobie określony czas na pracę. Jeśli masz problem z rozciągnięciem tego czasu, możesz zainstalować aplikację do zarządzania czasem lub wesprzeć się tzw. techniką Pomodoro, zakładającą podział pracy na 25-minutowe zadania. Aby zniwelować stres cyfrowy i zwiększyć swą produktywność w pracy, należy zdefiniować świadomy odpoczynek oraz określić funkcję narzędzi, z których korzysta się na co dzień. Model pracy zdalnej może wywoływać napięcia związane z nieustannym byciem dostępnym – dlatego tak istotne jest rozgraniczenie czasu pracy i czasu odpoczynku.

Jeśli wykorzystujesz smartfon zarówno do celów zawodowych, jak i prywatnych, kontroluj czas ogólnego użytkowania – pomocne mogą się okazać opcje w telefonach, tj. Cyfrowy Dobrostan (Android) czy ScreenTime (iOS). Miej świadomość, że smartfon zbiera bardzo dużo informacji nie tylko o Tobie, lecz także o Twojej organizacji. Bądź uważnym odbiorcą i nadawcą treści: gdy korzystasz ze służbowych mediów społecznościowych czy z poczty elektronicznej, nie klikaj w linki czy posty, które nie są związane z pracą.

Komentarz

Pamiętaj, że podstawą sprawnego funkcjonowania każdej organizacji jest człowiek. To on bywa najsłabszym ogniwem i ma największe skłonności do popełnienia błędu. Wszechobecna technologia, bez której już żadna organizacja nie jest w stanie efektywnie działać, tryb pracy zdalnej lub model hybrydowy mogą zachwiać równowagę pracowników pomiędzy życiem prywatnym a zawodowym. Brak znajomości podstawowych zasad higieny cyfrowej oraz nieumiejętność budowania zdrowych nawyków w kontekście technologii mogą skutkować negatywnym wpływem na zdrowie psychofizyczne, zaburzenia koncentracji, przeciążenie informacyjne czy zmniejszenie satysfakcji z pracy. To kolei stanowi realne zagrożenie dla całej organizacji. Zachowanie tech-life balance, a także świadome korzystanie z technologii w pracy i poza nią są zatem kluczowe.
// Sylwia Ryń, Fundacja Sarigato

Pamiętaj o mikronawykach związanych z cyberbezpieczeństwem 13

Rozwinięcie

- Nie zostawiaj sprzętu (służbowego czy prywatnego) bez nadzoru, a tym bardziej – bez blokady.
- Nie przyklejaj karteczek z hasłami do komputera czy na ścianę nad komputerem. Nie zapisuj ich również na pulpicie ani w notatniku telefonu.
- Zanim zainstalujesz jakąkolwiek aplikację, sprawdź, do jakich danych domaga się dostępu. Niektóre aplikacje mogą mieć wgląd m.in. do kalendarza, do kontaktów, do lokalizacji czy do mikrofonu.
- Nawyk związany z szyfrowaniem ważnych e-maili lub wysyłaniem ich w trybie poufnym jest szczególnie istotny. Pomyśl, co mogłoby się stać, gdyby zdarzyło Ci się wysłać wiadomość zawierającą informacje o umowach, grantach, projektach osobom postronnym.
- Twoja skrzynka e-mail to skarbnica wiedzy o Tobie i organizacji. Aby ją zabezpieczyć, stosuj weryfikację dwuetapową, a wszędzie tam, gdzie potrzebujesz zarejestrować się na chwilę, podawaj e-maile tymczasowe (www.tempt-mail.org).
- Gdy pracuje się w modelu zdalnym lub hybrydowym, łatwo udostępnić informacje o działalności organizacji przez przypadek. Zawsze miej świadomość, z kim i o czym rozmawiasz, a także – gdzie się aktualnie znajdujesz. Praca z kawiarni może być przyjemna, ale i niebezpieczna.

Komentarz

Aby zadbać o higienę cyfrową i o świadome korzystanie z technologii, czy to w pracy, czy – poza nią, warto wypracować kilka podstawowych mikronawyków związanych z cyberbezpieczeństwem. Ich wdrożenie uchroni Cię przed niepotrzebnym stresem związanym z utratą istotnych danych organizacji, dokumentów czy dostępów do kont. // Sylwia Ryń, Fundacja Sarigato

01 Rzetelność

02 Prawda

03 Bezpieczeństwo

04 Twórczość

INDID
Instytut Dyskursu
i Dialogu

Gdy publikujesz prace wykonane przez podopiecznych organizacji (np. rysunki czy zdjęcia), podpisz, kto jest ich autorem 01

Rozwinięcie

Warto zapytać autora pracy, czy nie ma nic przeciwko, aby publikowaną pracę podpisać jego imieniem i nazwiskiem. Pamiętaj, że autor ma również prawo do pozostania anonimowym.

Komentarz

Prawidłowy podpis dzieła zawiera: imię i nazwisko (lub pseudonim) autora, źródło, z którego pochodzi utwór, oraz rodzaj licencji, w ramach której ono zostało udostępnione. Np. „Dziewczyna z Gambii", fot: Ferdinand Reus, licencja: CC-BY-SA 2.0 // Iza Jania, Instytut Tyflologiczny Polskiego Związku Niewidomych

Przy publikacji zdjęć, na których znajdują się osoby, pamiętaj o ich prawie do ochrony wizerunku 02

Rozwinięcie

Zanim udostępnisz publicznie zdjęcie, które zawiera wizerunek osoby, powinieneś uzyskać jej zgodę na to. Najlepiej przygotować pisemną deklarację z wymienionymi celami, w których to zdjęcie zostanie wykorzystane.

Komentarz

Zgody nie wymaga rozpowszechnianie wizerunku osoby stanowiącej jedynie szczegół całości, np. zgromadzenie, krajobraz, publiczna impreza. Możesz to wykorzystać m.in., gdy robisz zdjęcia podczas szkolenia lub zajęć z oddali. *Np. Kosma Kołodziej, Diversity PL*

Pamiętaj, aby odróżniać umowę o dzieło od umowy zlecenia Specyfikacja UOD*:

03

ZUS	Warunki zwolnienia z obowiązku naliczenia składek na ubezpieczenie społeczne i zdrowotne.	URZĄD SKARBOWY

1. Umowa powinna wskazywać konkretny, samoistny, oznaczony rezultat, który ma postać postrzegalną, pozwalającą nie tylko odróżnić go od innych obiektów, lecz także uchwycić istotę osiągniętego rezultatu w postaci materialnej lub niematerialnej.
2. Rezultat ma mieć indywidulny charakter.
3. Nie może być związany z systematycznym wykonywaniem określonych czynności czy działań.
4. Wykonanie dzieła ma mieć charakter samodzielny i odbywać się bez nadzoru zamawiającego.
5. Dzieło powinno stanowić przejaw indywidualnej twórczości.
6. Dzieło powinno być wykonane z wykorzystaniem własnej wiedzy.
7. Dzieło powinno być wykonywane poza siedzibą firmy.

20%	Bez przekazania praw autorskich
50%	Z przekazaniem praw autorskich

OBOWIĄZEK SPRAWOZDAWCZY ZAMAWIAJĄCEGO

Zgłoszenie do ZUS informacji na druku RUD przez zamawiającego – płatnika składek w terminie 7 dni od zawarcia umowy.

Wymóg ten nie dotyczy podmiotów (np. stowarzyszeń, fundacji), które nie są zarejestrowane w ZUS jako płatnicy składek.

Wpłata do urzędu skarbowego zaliczki na podatek dochodowy od osób fizycznych w terminie do 20 dnia kolejnego miesiąca po wypłacie wynagrodzenia.

- PIT 11 do urzędu skarbowego do 31 stycznia następnego roku
- PIT 11 dla zleceniobiorcy do 28 lutego następnego roku
- PIT 4R do urzędu skarbowego do 31 stycznia następnego roku.

Sprawdzaj, czy zdjęcia, które zamierzasz wykorzystać, zostały wcześniej użyte (a jeśli tak, to na jakiej licencji) 04

Rozwinięcie

Może się zdarzyć, że zdjęcie (grafika), które chcesz wykorzystać, zostało oznaczone nieprawidłową licencją. Jest to rzadka sytuacja, ale może doprowadzić do sytuacji, w której nawet jeżeli pozostajesz w błędzie, naruszysz czyjeś autorskie prawa majątkowe i będziesz zobowiązany wypłacić odszkodowanie. Dlatego po wyborze zdjęcia (grafiki) warto sprawdzić, czy i na jakiej licencji zostało ono wcześniej użyte. Możesz to zrobić za pomocą wyszukiwania obrazem w wyszukiwarce Google.

Przy tworzeniu materiałów warto korzystać z oznaczeń Creative Commons 05

Rozwinięcie

Jeśli publikujesz materiały (raporty, scenariusze, sprawozdania), zastosuj licencje Creative Commons. Dzięki temu możesz z góry określić zasady, na jakich chcesz dzielić się z innymi efektami pracy Twojej organizacji. Licencje umożliwiają innym kopiowanie i rozpowszechnianie materiałów, przy czym możesz określić, czy ich wykorzystywanie może odbywać się wyłącznie na warunkach niekomercyjnych lub może ograniczyć możliwości tworzenia utworów zależnych. Oznacz wyraźną i prostą grafiką zasady tej licencji. Szczegóły na stronie Creative Commons.

Komentarz

Gdy korzystasz z grafiki udostępnionej na licencji CC, to oznaczenie licencji można umieścić w opisie np. treści posta (niekoniecznie na grafice, jeśli koliduje z kompozycją).

→ czytaj więcej na creativecommons.pl

Korzystaj w sposób legalny z pracy podopiecznych organizacji 06

Rozwinięcie

Jeśli zamierzasz wykorzystać pracę osoby uczestniczącej w zajęciach organizacji, np. do stworzenia logotypu projektu lub innej inicjatywy, pamiętaj, aby:

- zapytać o zgodę autora – jeśli jest to osoba pełnoletnia, uzyskaj jej pisemną zgodę na wykorzystanie utworu (jeśli nie, to zgodę powinni podpisać rodzice / opiekunowie prawni),
- oznaczyć autora podczas publikowania logotypu.

Gdy stosujesz prawo cytatu, wskaż konkretną podstawę prawną 07

Rozwinięcie

W utworach stanowiących samoistną całość wolno przytaczać urywki rozpowszechnionych utworów oraz rozpowszechnione utwory plastyczne, utwory fotograficzne lub drobne utwory w całości, w zakresie uzasadnionym celami cytatu, takimi jak: wyjaśnianie, polemika, analiza krytyczna lub naukowa, nauczanie, lub prawami gatunku twórczości. Gdy będziesz korzystać z prawa cytatu, możesz posłużyć się taką klauzulą:
„W ... (tytuł dzieła) wykorzystano na prawach cytatu fragmenty następujących utworów: ... w celu ... na podstawie art. 29 ustawy o prawie autorskim i prawach pokrewnych".

Chroń twórczość swojej organizacji 08

Rozwinięcie

W razie udostępniania dzieła stworzonego w ramach działalności Twojej organizacji (np. grafiki, sprawozdania) przez inne podmioty, przypominaj o konieczności oznaczenia lub podpisania autora dzieła i wskazania Twojej organizacji jako źródła pochodzenia tego dzieła. Warto mieć przygotowaną formułkę informacyjną, którą można wysłać w takiej sytuacji.

Korzystaj darmowych rozwiązań wspierających twórczość przeznaczonych dla NGO 09

Rozwinięcie

Skorzystaj z różnych rozwiązań i programów, m.in.:

Google dla organizacji non profit (G4NP) – darmowy pakiet od firmy Google, który ułatwia codzienną pracę i komunikację.

⟶ *czytaj więcej na google.com*

Canva dla organizacji non profit – darmowy program graficzny, który pozwala w łatwy sposób tworzyć podstawowe grafiki, np. na stronę internetową czy do mediów społecznościowych, a także pliki do wydruków, np. ulotki, plakaty.

⟶ *czytaj więcej na canva.com*

TechSoup – międzynarodowa sieć organizacji pozarządowych, która zapewnia wsparcie techniczne i narzędzia technologiczne innym organizacjom non profit.

⟶ *czytaj więcej na techsoup.pl*

Publikuj w otwartym dostępie 10

Rozwinięcie

Wydaną publikację (raport, sprawozdanie, broszurę) umieść w repozytorium (w miejscu przechowywania i udostępniania dokumentów) gromadzącym otwarte zasoby. Polskim repozytorium, w którym znajdują się publikacje trzeciego sektora, jest m.in. NGOteka.

⟶ *czytaj więcej na ngoteka.pl*

SOCNGO
Szkoła Odpowiedzialności Cyfrowej

Dziękujemy

za odpowiedzialne działanie w sieci

INDID
Instytut Dyskursu i Dialogu

DEMAGOG

Iceland Liechtenstein Norway Active citizens fund