DEKALOG

BEZPIECZEŃSTWA CYFROWEGO

CHRONI TWOJE DANE

KS. DANIEL BUDZIŃSKI

CHROŃ DANE OSOBOWE **POWIERZONYCH CI OSÓB**

Nie instaluj nieznanych programów
ani dodatków z niesprawdzonych źródeł.

PAMIĘTAJ

- Nie publikuj w internecie zdjęć dokumentów, list obecności, kart zgłoszeń, umów ani korespondencji zawierającej dane osobowe.
- Nie przesyłaj danych osobowych przez prywatne komunikatory. Korzystaj wyłącznie z zatwierdzonych i bezpiecznych kanałów komunikacji.
- Ogranicz dostęp do danych tylko do osób upoważnionych. Zbieraj i udostępniaj tylko te informacje, które są naprawdę potrzebne.
- W razie wysłania wiadomości do złego adresata lub wycieku danych natychmiast zgłoś incydent przełożonemu lub do IODa.

SPRAWDŹ

- [ ] Sprawdź, kto ma dostęp do komputerów, poczty elektronicznej, systemów kancelaryjnych i folderów z danymi.
- [ ] Sprawdź, gdzie przechowywane są dokumenty zawierające dane osobowe.
- [ ] Sprawdź, komu przekazywane są dane osobowe i na jakiej podstawie. Upewnij się, że udostępniany jest tylko niezbędny zakres danych.
- [ ] Czy masz włączoną automatyczną blokadę ekranu po kilku minutach bezczynności ?
- [ ] Zweryfikuj, czy istnieją procedury na wypadek zgubienia dokumentu, kradzieży laptopa lub wysłania danych do niewłaściwej osoby.

AKTUALIZUJ
SYSTEMY I OPROGRAMOWANIE

Regularne aktualizacje komputerów, telefonów i programów zabezpieczają przed znanymi lukami bezpieczeństwa oraz cyberatakami.

PAMIĘTAJ

- Włącz automatyczne aktualizacje w systemie Windows, macOS lub telefonie. Nie odkładaj instalacji poprawek „na później”.
- Regularnie aktualizuj przeglądarkę internetową, program antywirusowy i pakiet biurowy.
- Regularne aktualizacje usuwają luki bezpieczeństwa wykorzystywane przez cyberprzestępców.
- W organizacji wyznacz osobę odpowiedzialną za kontrolę aktualności sprzętu i oprogramowania.

SPRAWDŹ

- [ ] Upewnij się, że włączone są automatyczne aktualizacje.
- [ ] Sprawdź aktualność pakietów biurowych, przeglądarek internetowych, i innych programów i komunikatorów.
- [ ] Sprawdź, czy program antywirusowy jest aktywny i posiada aktualne bazy wirusów.
- [ ] Upewnij się, że skanowanie systemu odbywa się regularnie.
- [ ] Ustal harmonogram kontroli: np. raz w miesiącu przegląd wszystkich komputerów.

UŻYWAJ SILNYCH HASEŁ **I UWIERZYTELNIENIA**

Hasło powinno być długie,
unikalne i trudne do odgadnięcia.
Tam, gdzie to możliwe,
włącz logowanie dwuetapowe.

PAMIĘTAJ

- Twórz silne hasła – powinny być długie, unikalne i trudne do odgadnięcia. Nie używaj jednego hasła do wielu kont.
- Nie używaj imion, dat urodzenia ani prostych schematów. Nie udostępniaj osobom nieupoważnionym swoich danych logowania.
- Bezpieczne logowanie to obowiązek każdego pracownika i element ochrony danych osobowych.
- Natychmiast zgłaszaj podejrzenie przejęcia hasła lub nieautoryzowanego logowania.

SPRAWDŹ

- [ ] Sprawdź, czy hasła nie są zapisane na kartkach przy komputerze.
- [ ] Sprawdź, czy hasła są odpowiednio długie (12–14 znaków). Zweryfikuj, czy zawierają litery, cyfry i znaki specjalne.
- [ ] Włącz uwierzytelnianie (logowanie) wieloskładnikowe. Zweryfikuj, czy dodatkowy składnik logowania działa poprawnie (aplikacja, SMS).
- [ ] Upewnij się, że po odejściu pracownika dostęp do kont jest blokowany.
- [ ] Ustal harmonogram kontroli: np. raz w miesiącu przegląd wszystkich komputerów.

ZAWSZE WYLOGOWUJ SIĘ **PO ZAKOŃCZENIU PRACY**

Nie pozostawiaj otwartych kont i systemów bez nadzoru. Wylogowanie to prosta, ale skuteczna forma ochrony danych.

PAMIĘTAJ !

- Po zakończeniu pracy zamknij sesję w poczcie, systemach kadrowych, księgowych, bazach danych i panelach administracyjnych.
- Nawet krótkie odejście od biurka wymaga zablokowania ekranu lub wylogowania się z konta.
- Na komputerach wspólnych sprawdź, czy konto nie pozostało zalogowane oraz czy przeglądarka nie zapamiętała danych logowania.
- Traktuj wylogowanie jako codzienny nawyk bezpieczeństwa. aTo prosta czynność, która chroni dane przed dostępem osób nieuprawnionych.

SPRAWDŹ ?

- [ ] Czy komputer jest zablokowany lub wyłączony.
- [ ] Czy konto nie pozostało zalogowane automatycznie Sprawdź, czy nie jest aktywna opcja „zapamiętaj mnie” lub automatyczne logowanie.
- [ ] Czy nośniki danych zostały schowane. Sprawdź, czy pendrive, dysk zewnętrzny, karta pamięci nie zostały na biurku.
- [ ] Sprawdź ustawienia wygaszacza i blokady po kilku minutach bezczynności.
- [ ] Czy nikt nie korzysta z Twojego stanowiska. Upewnij się, że po odejściu nikt nie ma dostępu do Twojego konta lub komputera.

ZACHOWUJ OSTROŻNOŚĆ
PRZY OPERACJACH FINANSOWYCH

Sprawdzaj strony bankowe, certyfikaty bezpieczeństwa i dane odbiorców przelewów. Nigdy nie podawaj haseł ani kodów osobom podszywającym się pod instytucje.

PAMIĘTAJ !

- Korzystaj z zaufanego komputera, operacje finansowe wykonuj na służbowym lub prywatnym, odpowiednio zabezpieczonym urządzeniu.
- Loguj się przez bezpieczne połączenie. Sprawdź, czy strona banku lub systemu płatności korzysta z szyfrowania (https) i poprawnego adresu.
- Nie korzystaj z publicznych sieci Wi-Fi. Unikaj wykonywania przelewów w hotelach, galeriach handlowych czy kawiarniach. Stosuj VPN.
- Sprawdzaj komputer pod kątem nietypowych objawów. Wolne działanie, samoczynne okna, dziwne komunikaty lub przekierowania mogą oznaczać infekcję.

SPRAWDŹ ?

- [ ] Upewnij się, że osoby postronne nie widzą danych logowania ani szczegółów transakcji.
- [ ] Sprawdź, czy logujesz się na właściwą stronę banku lub systemu płatności oraz czy połączenie jest szyfrowane (https).
- [ ] Sprawdź, czy faktura, wiadomość e-mail lub polecenie przelewu pochodzi z wiarygodnego źródła.
- [ ] Po zakończeniu płatności wyloguj się z bankowości elektronicznej i zamknij przeglądarkę.
- [ ] Czy w przeglądarce nie ma podejrzanych dodatków.

CHROŃ DANE OSOBOWE **STRON INTERNETOWYCH**

Nie otwieraj nieznanych witryn bez sprawdzenia ich wiarygodności. Fałszywe strony często służą do wyłudzania danych lub instalacji wirusów.

PAMIĘTAJ

- Sprawdzaj dokładnie adres strony Zwracaj uwagę na literówki, dziwne znaki, dodatkowe słowa lub nietypowe domeny (nazwy stron).
- Unikaj klikania podejrzanych linków. Nie otwieraj odnośników z nieznanych e-maili, SMS-ów, komunikatorów ani reklam.
- Nie podawaj danych od razu. Jeśli strona prosi o hasło, dane osobowe lub płatność, najpierw potwierdź jej autentyczność.
- Zwracaj uwagę na wygląd strony i nie pobieraj plików z nieznanych witryn. Błędy językowe, niska jakość grafiki, chaos lub nietypowe komunikaty mogą świadczyć o oszustwie.

SPRAWDŹ

- [ ] Sprawdź, czy widoczne są wyłącznie informacje konieczne do realizacji celu publikacji.
- [ ] Czy pliki do pobrania nie zawierają ukrytych danych. Sprawdź PDF, Word i Excel pod kątem metadanych, komentarzy i historii zmian.
- [ ] Czy system strony jest aktualny. Sprawdź aktualizacje CMS, motywów, wtyczek i komponentów strony internetowej.
- [ ] Czy panel administracyjny jest zabezpieczony. Upewnij się, że dostęp mają tylko upoważnione osoby oraz stosowane są silne hasła.
- [ ] Zweryfikuj, czy archiwalne ogłoszenia, listy, galerie lub dokumenty nie ujawniają zbędnych danych.

UWAŻAJ NA **WIADOMOŚCI, LINKI I ZAŁĄCZNIKI**

Nie klikaj pochopnie w linki ani nie otwieraj plików od nieznanych nadawców.
To najczęstsza droga ataku phishingowego.

PAMIĘTAJ !

- Sprawdzaj nadawcę wiadomości. Zwracaj uwagę na adres e-mail, literówki w nazwie firmy lub nietypową domenę.
- Nie otwieraj załączników od nieznanych osób. Pliki z nieznanych źródeł mogą zawierać wirusy lub złośliwe oprogramowanie.
- Uważaj na pilne wezwania do działania. Wiadomości typu „natychmiast zapłać", „konto zostanie zablokowane" często są próbą oszustwa.
- Skanuj załączniki programem antywirusowym. Przed otwarciem pobranego pliku sprawdź go ochroną antywirusową.

SPRAWDŹ ?

- ☐ Czy temat wiadomości nie jest podejrzany. Zweryfikuj, czy temat nie wywołuje presji, strachu lub pośpiechu.
- ☐ Czy wiadomość żąda danych logowania. Sprawdź, czy nie prosi o hasło, kod SMS lub inne poufne informacje.
- ☐ Czy załącznik ma nietypową nazwę. Nazwy typu „faktura_12345.img" lub „skan.pdf.exe" mogą ukrywać złośliwy plik.
- ☐ Czy wiadomość zawiera zbyt atrakcyjną ofertę. Nagrody, zwroty pieniędzy, darmowe usługi lub promocje mogą służyć wyłudzeniu danych.
- ☐ Czy po kliknięciu strona zachowuje się normalnie. Nagłe pobieranie pliku, prośba o instalację dodatku lub wiele przekierowań budzi podejrzenia.

TWÓRZ
REGULARNE KOPIE ZAPASOWE

Backup dokumentów, baz danych i plików pozwala szybko odzyskać informacje po awarii, ataku ransomware lub błędzie użytkownika.

PAMIĘTAJ

- Oddziel kopię od komputera roboczego. Backup przechowuj na zewnętrznym nośniku, serwerze lub w bezpiecznej chmurze.
- Odłączaj dyski po wykonaniu kopii. Nośniki stale podłączone mogą zostać zaszyfrowane podczas ataku ransomware.
- Szyfruj kopie zapasowe. Chroń backup hasłem lub szyfrowaniem, szczególnie gdy zawiera dane osobowe.
- Chroń dostęp do backupów. Dostęp do kopii zapasowych powinny mieć tylko upoważnione osoby.

SPRAWDŹ

- [ ] Czy kopia znajduje się w bezpiecznej lokalizacji. Upewnij się, że backup jest zapisany poza komputerem roboczym – np. na serwerze, dysku.
- [ ] Czy kopie są chronione przed dostępem osób nieuprawnionych. Zweryfikuj hasła, uprawnienia i szyfrowanie backupów.
- [ ] Czy masz kopię najważniejszych plików. Sprawdź, czy dokumenty, zdjęcia i potrzebne foldery są zapisane także w innym miejscu.
- [ ] Sprawdź, czy przed większymi aktualizacjami wykonywana jest kopia zapasowa.
- [ ] Czy backup jest wykonywany regularnie. Sprawdź, czy kopie zapasowe są tworzone zgodnie z ustalonym harmonogramem.

WERYFIKUJ INFORMACJE
I NIE SZERZ DEZINFORMACJI

Sprawdzaj źródła wiadomości, szczególnie tych budzących emocje. Fałszywe informacje mogą szkodzić wspólnocie i reputacji instytucji.

PAMIĘTAJ !

- Korzystaj z oficjalnych kanałów komunikacji. Opieraj się na komunikatach ze strony internetowej, oficjalnych profilach.
- Porównuj wiadomość z innymi źródłami. Jeśli informacja jest prawdziwa, zwykle pojawia się także w innych wiarygodnych miejscach.
- Zachowaj ostrożność wobec treści budzących emocje. Wiadomości wywołujące strach, gniew lub oburzenie często mają skłonić do szybkiego udostępnienia.
- W razie wątpliwości zapytaj właściwą osobę. Skonsultuj informację z przełożonym, administracją lub osobą odpowiedzialną za komunikację.

SPRAWDŹ ?

- [ ] Czy znasz źródło informacji. Zweryfikuj adres e-mail, domenę oraz nazwę nadawcy komunikatu.
- [ ] Czy informacja o zagrożeniu jest potwierdzona. Porównaj komunikat z innymi zaufanymi źródłami bezpieczeństwa.
- [ ] Czy nie przekazujesz dalej niesprawdzonego ostrzeżenia. Nie rozsyłaj plotek o wirusach, atakach lub awariach bez potwierdzenia.
- [ ] Czy link prowadzi do bezpiecznej strony. Sprawdź adres strony przed kliknięciem i upewnij się, że nie jest podszyciem.
- [ ] Czy grafika lub logo nie są podrobione. Fałszywe komunikaty często używają nieaktualnych znaków firmowych lub niskiej jakości grafik.

UCZ SIĘ
I EDUKUJ INNYCH

Bezpieczeństwo cyfrowe wymaga stałej czujności. Aktualizuj wiedzę, śledź komunikaty KIOD o zagrożeniach i pomagaj szkolić pracowników parafii oraz instytucji kościelnych.

PAMIĘTAJ

- Regularnie aktualizuj swoją wiedzę. Śledź nowe zagrożenia, metody oszustw i zalecenia dotyczące cyberbezpieczeństwa.
- Bierz udział w szkoleniach. Uczestnicz w kursach, webinarach i spotkaniach dotyczących ochrony danych oraz bezpieczeństwa cyfrowego.
- Reaguj na błędy życzliwie i szybko. Gdy ktoś popełni błąd, pomóż naprawić sytuację i wyjaśnij, jak unikać podobnych zagrożeń.
- Przypominaj innym o podstawowych zasadach. Informuj współpracowników o silnych hasłach, MFA, phishingu i bezpiecznej pracy z danymi.

SPRAWDŹ

- [ ] Czy znasz aktualne zagrożenia. Sprawdź, czy jesteś na bieżąco z metodami phishingu, oszustw internetowych i wycieków danych.
- [ ] Czy przekazujesz wiedzę innym pracownikom. Upewnij się, że informujesz współpracowników o ważnych zagrożeniach i zasadach bezpieczeństwa.
- [ ] Czy nowe osoby są wdrażane w zasady bezpieczeństwa. Sprawdź, czy nowi pracownicy otrzymują podstawowe instrukcje i szkolenie.
- [ ] Czy wiesz, komu zgłosić incydent.
- [ ] Czy sam stosujesz dobre praktyki. Upewnij się, że dajesz przykład innym: używaj silnych haseł, MFA i zachowuj ostrożność online.

NAJWAŻNIEJSZE ZABEZPIECZENIE **ZDROWY ROZSĄDEK**

Nawet najlepszy antywirus, firewall czy hasło nie ochronią przed pochopnym kliknięciem w podejrzany link, podaniem danych oszustowi czy zignorowaniem podstawowych zasad bezpieczeństwa.

PAMIĘTAJ

Każdy pracownik, IOD, KIOD oraz administrator danych powinien pamiętać, że **najważniejszym zabezpieczeniem jest człowiek** – jego **zdrowy rozsądek, spokój i opanowanie**. Nawet najlepszy antywirus, firewall, silne hasło czy nowoczesny system ochrony nie zastąpią czujności użytkownika. Wiele incydentów zaczyna się od pośpiechu, rutyny, nieuwagi albo jednego pochopnego kliknięcia w podejrzany link.

Ryzyko w świecie cyfrowym istnieje zawsze i wszędzie, dlatego nie chodzi o to, aby się go bać, lecz aby **umieć nim rozsądnie zarządzać**. Spokojna analiza sytuacji, weryfikacja wiadomości, ostrożność przy logowaniu, płatnościach czy udostępnianiu danych często znaczą więcej niż kosztowne narzędzia techniczne.

W praktyce warto pamiętać o kilku prostych zasadach: zatrzymaj się, zanim klikniesz; sprawdzaj nadawcę i źródło informacji; nie działaj pod presją czasu; pytaj, gdy masz wątpliwości; zgłaszaj podejrzane sytuacje; stosuj podstawowe procedury bezpieczeństwa każdego dnia.

Cyberbezpieczeństwo zaczyna się nie w komputerze, lecz w głowie użytkownika. To właśnie rozwaga, czujność i dobre nawyki są pierwszą i najskuteczniejszą linią obrony.