INFORMACJA O CYBERBEZPIECZEŃSTWIE

Realizując zadania, wynikające z art. 22 ust. 1 pkt 4 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, przekazujemy Państwu informacje pozwalające zrozumieć zagrożenia występujące w cyberprzestrzeni oraz porady jak skuteczne stosować sposoby zabezpieczenia się przed tymi zagrożeniami.

Cyberbezpieczeństwo, to zgodnie z treścią art. 2 pkt 4 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa - ***„odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy”.***

Do najpopularniejszych zagrożeń w cyberprzestrzeni, z którymi mogą się Państwo spotkać, należą:

- ataki z użyciem szkodliwego oprogramowania *(malware, wirusy, robaki, itp.),*
- kradzieże tożsamości,
- kradzieże *(wyłudzenia),* modyfikacje bądź niszczenie danych,
- blokowanie dostępu do usług,
- spam (niechciane lub niepotrzebne wiadomości elektroniczne),
- ataki socjotechniczne (np. *phishing, czyli wyłudzanie poufnych informacji przez podszywanie się pod godną zaufania osobę lub instytucję).*

Sposoby zabezpieczenia się przed zagrożeniami:

- Stosuj zasadę ograniczonego zaufania do odbieranych wiadomości e-mail, sms, stron internetowych nakłaniających do podania danych osobowych, osób podających się za przedstawicieli firm, instytucji, którzy żądają podania danych autoryzacyjnych lub nakłaniających do instalowania aplikacji zdalnego dostępu. Pamiętaj, że żaden bank czy Urząd nie wysyła e-maili do swoich klientów / interesantów z prośbą o podanie hasła lub loginu w celu ich weryfikacji.
- Nie ujawniaj danych osobowych w tym danych autoryzacyjnych dopóki nie ustalisz czy rozmawiasz z osobą uprawnioną do przetwarzania twoich danych.
- Staraj się nie odwiedzać zbyt często stron, które oferują niesamowite atrakcje *(darmowe filmiki, muzykę, albo łatwy zarobek przy rozsyłaniu spamu*) – często na takich stronach znajdują się ukryte wirusy, trojany i inne zagrożenia.
- Instaluj aplikacje tylko ze znanych i zaufanych źródeł.
- Nie otwieraj wiadomości e-mail i nie korzystaj z przesłanych linków od nadawców, których nie znasz.
- Każdy e-mail można sfałszować, sprawdź w nagłówku wiadomości pole Received: from *(ang. otrzymane od).* W tym polu znajdziesz rzeczywisty adres serwera nadawcy.
- Szyfruj dane poufne wysyłane pocztą elektroniczną. Nie wysyłaj w e-mailach żadnych poufnych danych w formie otwartego tekstu. Stosuj szyfrowanie plików za pomocą np.: 7zip lub zabezpiecz tekst hasłem.
- Bezpieczeństwo wiadomości tekstowych (SMS). – sprawdź adres url, z którego domyślnie dany podmiot / instytucja wysyła do ciebie smsy. Cyberprzestępca może podszyć się pod dowolną tożsamość (*odpowiednio definiując numer lub nazwę*),

otrzymując sms-a, w którym cyberprzestępca podszywa się pod numer zapisany w książce adresowej, telefon zidentyfikuje go jako nadawcę wiadomości sms.

- Jeśli na podejrzanej stronie podałeś swoje dane do logowania lub jeżeli włamano się na twoje konto e-mail – jak najszybciej zmień hasło.
- Chroń swój komputer, urządzenie mobilne programem antywirusowym zabezpieczającym przez zagrożeniami typu; wirusy, robaki, trojany, niebezpiecznymi aplikacjami typu ransomware, adware, keylogger, spyware, dialer, phishing, narzędziami hakerskimi, backdoorami. rootkitami, bootkitami i exploitami.
- Aktualizuj system operacyjny, aplikacje użytkowe, programy antywirusowe, brak aktualizacji zwiększa podatność na cyberzagrożenia. Hakerzy, którzy znają słabości systemu / aplikacji, mają otwartą furtkę do korzystania z luk w oprogramowaniu.
- Logowanie do e-usług publicznych, bankowości elektronicznej bez aktualnego (*wspieranego przez producenta)* systemu operacyjnego to duże ryzyko.
- Korzystaj z różnych haseł do różnych usług elektronicznych.
- Tam gdzie to możliwe (*konta społecznościowe, konto e-mail, usługi e-administracji, usługi finansowe)* stosuj dwuetapowe uwierzytelnienie za pomocą np. sms, pin, aplikacji generującej jednorazowe kody autoryzujące, tokenów, klucza fizycznego.
- Regularnie zmieniaj hasła.
- Nie udostępniaj nikomu swoich haseł.
- Pracuj na najniższych możliwych uprawnieniach użytkownika.
- Pamiętaj o uruchomieniu firewalla.
- Wykonuj kopie bezpieczeństwa. *(kopie możesz wykonać na dysku przenośnym np.: pendrive – pamiętaj, aby dysk zabezpieczyć hasłem. Zrobisz to za pomocą aplikacji Bitlocker).*
- Skanuj podłączane urządzenia zewnętrzne.
- Skanuj regularnie wszystkie dyski twarde zainstalowane na twoim komputerze.
- Kontroluj uprawnienia instalowanych aplikacji.
- Unikaj z korzystania otwartych sieci Wi-Fi.

Zrozumienie zagrożeń cyberbezpieczeństwa i stosowanie sposobów zabezpieczania się przed zagrożeniami to wiedza niezbędna każdemu użytkownikowi komputera, smartphona czy też usług internetowych. Wszelkie porady bezpieczeństwa dla użytkowników tych urządzeń dostępne są na:

- Witrynie internetowej CSIRT NASK – Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego działającego na poziomie krajowym pod adresem: https://www.cert.pl
- Witrynie internetowej Ministerstwa Cyfryzacji pod adresem: https://www.gov.pl/web/cyfryzacja/cyberbezpieczenstwo
- NASK – państwowy instytut badawczy nadzorowanym przez Kancelarię Prezesa Rady Ministrów – https://www.nask.pl/
- **STÓJ. POMYŚL. POŁĄCZ.** jest polską wersją międzynarodowej kampanii STOP. THINK. CONNECT.™, mającej na celu zwiększanie poziomu świadomości społecznej i promowanie bezpieczeństwa w cyberprzestrzeni. Zapoznaj się z dobrymi praktykami opublikowanymi na stronach kampanii oraz z dostępnymi na niej materiałami do pobrania. Na stronie internetowej kampanii można zapoznać się z dobrymi praktykami, jak również z innymi materiałami i wskazówkami: **https://stojpomyslpolacz.pl/stp/dobre-praktyki**
- **OUCH!** To cykliczny, darmowy zestaw porad bezpieczeństwa dla użytkowników komputerów. Każde wydanie zawiera krótkie, przystępne przedstawienie wybranego

zagadnienia z bezpieczeństwa komputerowego wraz z listą wskazówek jak można chronić siebie, swoich najbliższych i swoją organizację. Zobacz wszystkie polskie wydania **OUCH!** na stronie CERT Polska. Z polską wersją Biuletynu można zapoznać się na stronie zespołu CERT Polska znajdującej się w strukturze Państwowego Instytutu Badawczego NASK (Naukowej i Akademickiej Sieci Komputerowej) pod adresem **https://www.cert.pl/ouch/.**

- Zespół **CERT Polska** działa w strukturach NASK (Naukowej i Akademickiej Sieci Komputerowej) – państwowego instytutu badawczego prowadzącego działalność naukową, krajowy rejestr domen .pl i dostarczającego zaawansowane usługi teleinformatyczne. CERT Polska jest zespołem specjalistów zwalczających zagrożenia w sieciach komputerowych. Zapoznaj się z **rocznymi raportami z działalności CERT Polska** zawierającymi zebrane dane o zagrożeniach dla polskich użytkowników Internetu, w tym również opisy najciekawszych nowych zagrożeń i podatności. Raporty dostępne są pod adresem **https://www.cert.pl/publikacje/.**

Dodatkowo zachęcamy do zapoznania się z poradnikami:

- **https://www.saferinternet.pl/materialy-edukacyjne/poradniki-i-broszury.html**
- **https://akademia.nask.pl/materialy.html**
- zestaw porad bezpieczeństwa dla użytkowników komputerów prowadzony na witrynie internetowej CSIRT NASK – Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego działającego na poziomie krajowym: **https://www.cert.pl/ouch/**
- poradniki na witrynie internetowej Ministerstwa Cyfryzacji:**https://www.gov.pl/web/baza-wiedzy/cyberbezpieczenstwo**
- publikacje z zakresu cyberbezpieczeństwa: **https://www.cert.pl/**

Zgłaszanie incydentów bezpieczeństwa: https://incydent.cert.pl/

Na osobę odpowiedzialną za utrzymywanie kontaktów z podmiotami Krajowego Systemu Cyberbezpieczeństwa w zakresie zadań publicznych zależnych od systemów informacyjnych, wyznaczony został Roman Frąckowiak, który w Szkole Podstawowej im. Wojska Polskiego w Mroczy pełni również zadania Inspektora Ochrony Danych Osobowych.

Dane kontaktowe do koordynatora ds. cyberbezpieczeństwa:
e-mail: kontaktkscfrackowiak1@gmail.com
tel.: 531-692-571

Przydatne informacje w zakresie cyberbezpieczeństwa:

- Zapoznaj się z poradnikiem dotyczącym bezpieczeństwa skrzynek pocztowych i kont w mediach społecznościowych oraz zastosuj się do jego rekomendacji.
- Bądź wyczulony na sensacyjne informacje, w szczególności zachęcające do natychmiastowego podjęcia jakiegoś działania. Weryfikuj informacje w kilku źródłach. **Upewnij się, że informacja jest prawdziwa przed podaniem jej dalej w mediach społecznościowych. Jeśli masz jakieś wątpliwości, wstrzymaj się.**
- Uważaj na wszelkie linki w wiadomościach mailowych i SMS-ach, zwłaszcza te sugerujące podjęcie jakiegoś działania, np. konieczność zmiany hasła, albo podejrzaną aktywność na koncie. Obserwowaliśmy w przeszłości tego typu celowane ataki na prywatne konta, gdzie celem było zdobycie informacji zawodowych.

- Upewnij się, że posiadasz kopię zapasową wszystkich ważnych dla siebie plików i potrafisz je przywrócić w przypadku takiej potrzeby.
- Śledź ostrzeżenia o nowych scenariuszach ataków na naszych mediach społecznościowych: Twitter, Facebook.
- Zgłaszaj każdą podejrzaną aktywność przez formularz na stronie incydent.cert.pl lub mailem na cert@cert.pl. Podejrzane SMS-y prześlij bezpośrednio na numer **799 448 084. Rekomendujemy zapisanie go w kontaktach.**

Teraz jeszcze łatwiej zgłosić incydent bezpieczeństwa - przez SMS

"Wymagana dopłata do paczki" czy ***"odbiór środków od kupującego"*** - takie wezwania często pojawiają się w wiadomościach wysyłanych przez oszustów, którzy próbują wyłudzić od nas pieniądze. Każdego takiego SMS-a warto zgłosić do CSIRT NASK.

Teraz można to zrobić jeszcze łatwiej, używając w swoim telefonie funkcji "przekaż" albo "udostępnij" i przesyłając treść otrzymanej wiadomości na numer 799-448-084. Trafi ona do analityków CERT Polska, którzy zdecydują o dopisaniu podejrzanej domeny do listy ostrzeżeń. Każde zgłoszenie może pomóc ochronić tysiące innych użytkowników!

Pamiętaj:

* Zapisz numer **799-448-084** w telefonie, aby mieć go zawsze pod ręką.
* Z jednego numeru możesz zgłosić maksymalnie 3 wiadomości w ciągu 4 godzin.
* Każde zgłoszenie jest dokumentowane i weryfikowane przez operatorów CERT Polska.
* Numer służy do zgłaszania prób wyłudzeń internetowych (phishingu, fałszywych aplikacji) - nie dotyczących usług SMS premium.
* Przekaż całą wiadomość w oryginalnej formie - nie wycinaj odnośnika ani treści.
* Więcej o liście ostrzeżeń CERT Polska, na która trafiają zgłaszane domeny, można przeczytać na stronie https://cert.pl/posts/2020/03/ostrzezenia_phishing/

W przypadku otrzymania podejrzanej wiadomości, warto zgłosić ją jak najszybciej!

CERT Polska (www.cert.pl) realizuje zadania na poziomie operacyjnym w trybie 24/7/365 przyjmując, wstępnie analizując i adresując zgłoszenia. Podejmuje działania i koordynuje reakcje na incydenty dotyczące bezpieczeństwa cywilnej cyberprzestrzeni RP zgłaszane przez operatorów usług kluczowych, dostawców usług cyfrowych, samorząd terytorialny i osoby prywatne. Od dnia 28 sierpnia 2018 r. zespołowi CERT Polska zostały powierzone obowiązki CSIRT NASK wynikające z ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

Jak chronić dane osobowe?

Dane osobowe, są bardzo cenne, bo dzięki nim można uzyskać dostęp do wielu dóbr. Mogą one też być wykorzystywane w celach marketingowych i sprzedażowych czy także, niestety, w celach przestępczych. Aby lepiej chronić dane osobowe każdej osoby i bezpiecznie je przetwarzać w Unii Europejskiej obowiązują specjalne przepisy, które temu służą. To ogólne rozporządzenie o ochronie danych (RODO).

Urząd Ochrony Danych Osobowych opracował najważniejsze porady, w jaki sposób zadbać o swoje dane osobowe:

1. Uważaj, co i komu udostępnisz o sobie w Internecie

Zdarza się, że nadmiernie dzielisz się informacjami na swój temat, a w mediach społecznościowych dzielisz się informacjami o sobie, o swoim stanie majątkowym, miejscu pracy, wydarzeniach ze swojego codziennego życia. Udostępniasz swoją lokalizację, wrzucasz zdjęcia. Przez to Internet jest źródłem wiedzy także o twoich poglądach, zachowaniach, konsumenckich zainteresowaniach. Dane te pozwalają, np. działom marketingowym różnych firm, dostosować ofertę kierowaną do ciebie. Ale też z takich informacji mogą skorzystać oszuści w celach przestępczych. Szczególnie, gdy profil który ciebie dotyczy jest w pełni publiczny, możesz być narażony na użycie twoich danych bez twojej wiedzy i przyzwolenia niezgodnie z celami, dla których dane udostępniłeś.

2. Nie zostawiaj dokumentów w zastaw

Zgodnie z prawem zatrzymywanie dowodu osobistego, czy paszportu bez podstawy prawnej jest karane. Utrata kontroli nad dowodem osobistym czy paszportem naraża ciebie na posłużenie się tym dokumentem bez twojej wiedzy i woli, co z kolei stwarza niebezpieczeństwo kradzieży tożsamości.

3. Nie pozwól robić kopii

Co do zasady nie powinieneś się godzić na kopiowanie twojego dokumentu tożsamości. Tylko w niektórych sytuacjach jest to wyjątkowo dopuszczalne gdy pozwalają na to przepisy prawa *(np. banki, spółdzielcze kasy oszczędnościowo-rozliczeniowe, czy tez krajowe instytucje płatnicze na podstawie: Prawo bankowe, czy przepisów o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu).* Gdy Administrator Danych Osobowych domaga się kopii np. twojego dowodu osobistego, poproś, aby wskazał tobie podstawę prawną, która nakłada na niego obowiązek takiego działania.

W innych wypadkach, jak np. wypożyczenie sprzętu – nie gódźmy się na to. Taka praktyka naraża nas na niebezpieczeństwo utraty danych osobowych.

4. Nie podawaj danych przez telefon

Unikaj przekazywania danych telefonicznie – szczególnie, gdy to nie ty inicjujesz rozmowę, ale ktoś dzwoni do ciebie. Udostępnianie danych na odległość obarczone jest ryzykiem, brakiem pewności co do tego komu faktycznie dane są przekazane.

Upewnij się, komu faktycznie udostępniasz dane w trakcie rozmowy telefonicznej, a jeżeli trzeba zweryfikuj kontakt, np. oddzwaniając i sprawdzając, czy dany numer i osoba faktycznie reprezentuje podmiot, na który się powołała.

5. Uważaj na różne formularze, poprzez które udostępniasz dane

Zachowaj rozwagę przy wypełnianiu i podpisywaniu różnego rodzaju ankiet, formularzy czy umów. Zastanów się, czy faktycznie chcesz założyć kartę lojalnościową w sklepie, by mieć rabaty lub dodatkowe promocje. W takich sytuacjach podajesz sklepom imię, nazwisko, adres zamieszkania, datę urodzenia, adres e-mail, numer telefonu, a w zamian otrzymujesz promocje, bony rabatowe, dodatkowe upominki przy zakupach – zastanów się, czy rabat, który otrzymasz jest tego wart.

Należy pamiętać, że Administrator Danych osobowych musi spełnić wobec ciebie obowiązek informacyjny, czyli przekazać tobie niezbędne informacje na swój temat, podając m.in. swoją tożsamość, dane kontaktowe oraz dane kontaktowe swojego inspektora ochrony danych osobowych *(o ile go wyznaczył),* po co, czyli w jakim celu i na jakiej podstawie prawnej przetwarza twoje dane.

6. Unikaj podawania nadmiarowych danych

Nie podawaj wszelkich danych *(danych nadmiarowych),* które pozwalają na pełną identyfikację, jeżeli w danej sytuacji nie jest to konieczne. Jeśli musisz skorzystać z danej usługi, to podaj tylko dane niezbędne do jej wykonania – dobrze przemyśl przekazanie tych danych, których przekazanie oznaczone jest jako opcjonalne.

7. Wyrażam zgodę na…

Zanim zaznaczysz wszystkie zgody pozwalające na przetwarzania twoich danych osobowych, upewnij się czego dotyczą. Zwróć uwagę, czy w formularzu zgody nie są zaznaczone one w sposób domyślny.

Dokładnie też czytaj, czego dotyczą klauzule zgód. Do każdej zgody musi być osobna klauzula informacyjna. W przypadku wątpliwości, zadawaj pytania Administratorom Danych Osobowych. Powinni ciebie poinformować o okresie przez jaki dane będą przetwarzane oraz o przysługujących tobie prawach, w tym dostępu do danych, ich sprostowania, usunięcia czy wniesienia sprzeciwu wobec przetwarzania, a także, czy twoje dane będą komuś innemu *(innym odbiorcom)* przekazywane.

Pamiętaj, że często udzielasz zgód na wykorzystywanie danych w celach marketingowych nie tylko przez danego Administratora Danych Osobowych, ale i jego partnerów biznesowych. O ile możesz, zweryfikuj, kim oni są, jakie to są firmy. Zgody na marketing „cudzy" powinny być nieobowiązkowe, powinna być ci pozostawiona możliwość wyboru co do tego, czy taką zgodę wyrazisz.

Administrator Danych Osobowych powinien zapewnić tobie, by możliwość wycofania zgody była równie łatwa, jak jej udzielenie oraz powinieneś być poinformowany o prawie do cofnięcia zgody, po tym jak ją wyrazisz.

8. Nie wyrzucaj danych do śmieci, dopóki ich nie zniszczysz

Wszelkie dokumenty z twoimi danymi, to kolejne źródło wiedzy o tobie, zwłaszcza gdy zawierają one wiele różnych informacji umożliwiających wyciągania wniosków na twój temat. Dlatego też – zanim wyrzucisz dokumenty do kosza – należy je zniszczyć *(np. faktury, rachunki, zapiski, naklejki na opakowaniach od korespondencji czy po dostarczonych towarach),* w sposób uniemożliwiający odtworzenie zawartych w nich danych osobowych.

9. Usuwaj trwale dane z nośników

Ogrom danych o tobie może znajdować się na twoich starych dyskach twardych, kartach pamięci, pendrive'ach czy innych nośnikach. Zwróć uwagę, że coraz więcej informacji na twój temat jest zapisanych w komputerach, smartfonach, aparatach fotograficznych czy tabletach. Zanim się pozbędziesz takich urządzeń lub nośników, trwale

usuń z nich dane. Jednak zwykłe ich skasowanie nie będzie wystarczające, gdyż wiele danych da się odzyskać. Dlatego zanim wyrzucisz nośnik albo go sprzedasz, usuń z niego dane, korzystając przy tym z odpowiedniego do tego oprogramowania. Warto też przywrócić ustawienia fabryczne urządzenia, aby nie było w nim zapamiętanych loginów i haseł do różnych usług i aplikacji, z jakich korzystałeś, a zwłaszcza z takich, z których nadal korzystasz.

10. Używaj programów chroniących urządzenia mobilne

Używaj oprogramowania chroniącego urządzenia mobilne, np. smartfon czy komputer, przed niepożądanymi działaniami z zewnątrz, np. złośliwego oprogramowania. Oprócz popularnych programów antywirusowych przydatne mogą być również te, które zabezpieczą przed ingerencją z zewnątrz tzw. firewall. Ważna jest bieżąca aktualizacje. Złośliwe oprogramowanie, przed którym chronią nas takie narzędzia, powstaje codziennie.

11. Unikaj publicznych hotspotów

Należy unikać „otwartych" hotspotów dostępnych dla wszystkich w zatłoczonych miejscach. W przypadku korzystania z sieci w hotelu lub kawiarni należy upewnić się czy punkt dostępu, do którego się logujemy, na pewno należy do miejsca, w którym właśnie przebywamy. Jeśli nie mamy pewności, ograniczmy się do wyszukiwania informacji i nie korzystajmy z usług, które wymagają podania hasła. Należy ograniczyć się do korzystania wyłącznie ze stron internetowych obsługujących protokół HTTPS lub używając tunelu VPN.

12. Zadbaj o hasła

Dobrze jest, aby nie miały one nic wspólnego z twoimi życiem osobistym, miejscem zamieszkania, twoim imieniem i nazwiskiem, datą urodzin, imionami twoich bliskich czy twoich zwierząt itp., tj. informacjami, które łatwo można skojarzyć z tobą obserwując twoje zachowania w sieci, czy połączyć z innymi informacjami o tobie.

Nie powinno się też zapisywać ich na kartce papieru czy w notesie. Najlepiej jest je zapamiętywać, co jest dużą sztuką, gdy musimy logować się do wielu serwisów. Pomocne w tym zakresie mogą być np. darmowe menadżery haseł, które umożliwiają nie tylko generowanie odpowiednio trudnych do złamania haseł, ale i zapamiętują je za nas. Tym samym łatwiejsza jest częstsza zmiana haseł, a ryzyko, że ktoś je pozna maleje.

Na bieżąco zmieniaj hasła dostępu do swojego komputera, do poczty elektronicznej, systemów bankowości elektronicznej, ale nawet sklepów internetowych, w których masz konto użytkownika. Staraj się przy tym korzystać z różnych haseł.

13. Wprowadź uwierzytelnianie wieloskładnikowe

Uwierzytelnianie wieloskładnikowe jest niezbędne, gdyż zapewnia dodatkową ochronę podczas logowania. Podczas uzyskiwania dostępu, oprócz wpisania hasła, użytkownicy muszą przejść dodatkową weryfikację tożsamości, np. poprzez wprowadzenie kodu otrzymanego na numer telefonu.

14. Uważaj na ogłoszenia

Przykładem sytuacji, gdy jesteśmy narażeni na utratę danych jest poszukiwanie pracy. Niestety, wśród prawdziwych ogłoszeń są i takie, których celem jest pozyskanie jak najdokładniejszych informacji na nasz temat. Warto więc bardzo dokładnie analizować takie treści i szczególną ostrożność zachować, gdy potencjalny pracodawca chce byśmy oprócz podstawowych danych na swój temat i wskazania danych do kontaktu, także np. udostępnili skany naszych dokumentów tożsamości, **co nie jest niezbędne w procesie rekrutacji**. Warto korzystać z oficjalnych serwisów pośrednictwa pracy.

15. Bądź czujny / czujna

Zachowaj ostrożność, która może uchronić twoje dane osobowe przed dostaniem się w ręce nieupoważnionych podmiotów lub osób, gdyż wśród nich mogą znaleźć się takie *(np. grupy przestępcze, złodzieje, porywacze),* które pozyskane w ten sposób informacje wykorzystają niezgodnie z prawem.

- Nie odpowiadaj na e-maile od osób, których nie znasz, zwłaszcza gdy domagają się podania jakichś informacji o tobie czy namawiają do kliknięcia w przesłany link lub otwarcia przesłanego załącznika, sugerują zmianę identyfikatora i hasła.
- Zachowaj ostrożność także przy korzystaniu z usług bankowości elektronicznej i dokonywaniu zakupów przez Internet.
- Zwracaj uwagę, czy aby na pewno logujesz się do serwisu bankowości internetowej ze strony banku, która ma certyfikat SSL *(widoczny w pasku adresu przeglądarki).*
- Weryfikuj sklepy, w których chcesz coś kupić: czy w ogóle istnieją, czy i jakie mają opinie, czy są to podmioty zidentyfikowane, gdzie mają siedzibę, czy podany jest kontakt z ich właścicielem i czy kontakt ten nie jest ograniczony tylko do elektronicznego. Jeśli masz wątpliwości co do bezpieczeństwa swoich danych zastanów się, czy koniecznie musisz dokonać zakupów u tego sprzedawcy.
- Weryfikuj regulaminy i polityki prywatności – unikaj sprzedawców nieprzedstawiających takich dokumentów, czy też prezentujących w nich postanowienia zbyt ogólne, niejasno czy nieprecyzyjnie brzmiące, sformułowane niepoprawnie gramatycznie czy językowo, może to bowiem oznaczać, że są to podmioty niepodlegające polskiemu czy europejskiemu prawu.

Ochrona danych osobowych jest bardzo ważna. Odpowiednio chroniąc swoje dane osobowe, możesz ograniczyć ryzyko ich wykorzystania przez osoby do tego nieuprawnione.