Networking Academy

SZKOŁY EKONOMICZNO-HANDLOWE
MACIERZ SZKOLNA W GDAŃSKU E.V.
im. Macierzy Szkolnej w Gdańsku

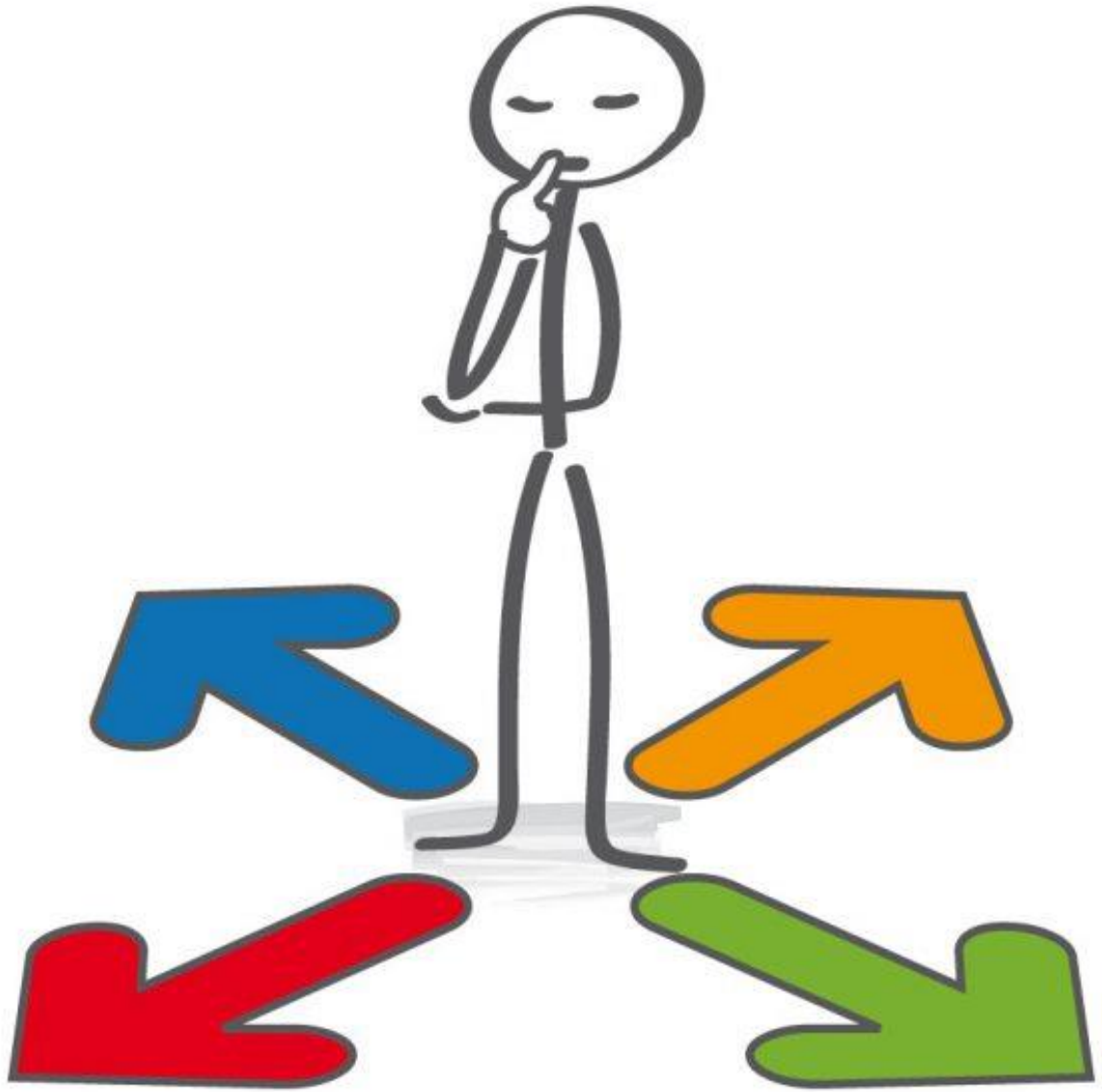
BEZPIECZNE FINANSE W SIECI…

Uczymy się od siebie dla siebie.

BEZPIECZEŃSTWO W SIECI

Bezpieczeństwo- jest to uczucie, którego każdy chce doświadczać.
Wielu ludzi nie zdaje sobie sprawy z tego,
że przebywając w sieci nie są tak bezpieczni jak im się wydaje.

W świecie wirtualnym sami musimy zadbać o swoje bezpieczeństwo oraz o to, by nasze prywatne życie nie stało się celem czyhających tam zagrożeń.



OD CZEGO NALEŻY ZACZĄĆ?

1. SIEĆ WLAN, LAN CZY WIFI?

WLAN- Wireless Local Area Network, to najczęściej spotykana domowa sieć bezprzewodowa - jest bezprzewodowym (Wireless) LAN-em, czyli grupą połączonych ze sobą komputerów, pozostających w niewielkiej odległości od siebie. Sieci LAN stosowane są w wielu domach, szkołach i firmach. Mimo że możliwe jest posiadanie więcej niż jednego LAN w domu, mało kto się na takie rozwiązania decyduje. Urządzenia połączone ze sobą taką siecią wykorzystują mikrofale w charakterze medium przenoszącego sygnały. Używają także podczerwieni.

WiFi to ZNAK TOWAROWY ☺ Nazwa używana jest do sygnowania urządzeń opartych na jednakowych standardach IEEE 802.11, pozwalających na korzystanie z sieci bezprzewodowych. Znak towarowy WiFi jest własnością firmy WiFi Alliance. Urządzenie oznaczone znakiem WiFi jest gotowe do pracy w sieci WLAN.

W Polsce przyjęło się traktować pojęcia „WLAN" i „WiFi" jako synonimy - w rzeczywistości określają dwie różne kwestie, choć w praktyce dotyczą tego samego.

ZAPAMIĘTAJ ☺

Sieci publiczne ("darmowe" Wi-Fi) zazwyczaj NIE posiadają odpowiednio wysokich zabezpieczeń, dlatego gdy jesteśmy do nich podłączeni, nie powinniśmy wykonywać internetowych płatności lub logować się na strony banku.

2. BEZPIECZNE STRONY TO PODSTAWA

Należy korzystać tylko i wyłącznie ze sprawdzonych oraz bezpiecznych stron internetowych.

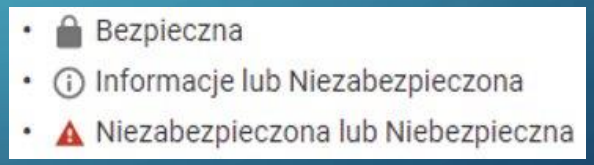
„Podejrzane strony" odpalane najczęściej są poprzez fałszywe serwery (DNS), mogą zawierać różnego typu wirusy, złośliwe oprogramowania oraz programy szpiegujące, które mogą wykraść nasze prywatne dane.

JAK SPRAWDZIĆ BEZPIECZEŃSTWO STRONY?

Zwróć uwagę na certyfikat bezpieczeństwa– po wejściu na stronę internetową w pasku wyszukiwarki powinno wyświetlać się https://

Jeżeli widnieje tylko http:// sklep może nie posiadać certyfikatu bezpieczeństw SSL i pewnie część zasobów jest niezabezpieczona.

- **Możemy łatwo sprawdzić bezpieczeństwo strony internetowej w przeglądarce.**
- **Popatrz na symbol stanu bezpieczeństwa na lewo od adresu internetowego.**



- **By zobaczyć szczegóły i uprawnienia strony, kliknij ikonę. Zobaczysz podsumowanie informacji o stopniu prywatności połączenia.**

CO TO JEST PHISING?

Metoda oszustwa, w której przestępca podszywa się pod inną osobę lub instytucję w celu wyłudzenia poufnych informacji, np. danych logowania, danych karty kredytowej,

zainfekowania komputera szkodliwym oprogramowaniem, czy też nakłonienia ofiary do dokonania określonych działań.

3. BEZPIECZNE LOGOWANIE

BEZPIECZNE HASŁO

Jest skomplikowane- zawiera małe i duże litery, cyfry oraz znaki specjalne, np. BaS01#@xyz!%

Nie odnosi się do danych, które można łatwo zdobyć o Tobie przeszukując sieć, portale społecznościowe itp.

Korzystaj z dwuskładnikowego uwierzytelniania logowania (sms na telefon).

ZAPAMIĘTAJ ☺

- ✓ Używaj różnych haseł do różnych stron, dzięki temu zminimalizujesz zagrożenie utraty danych i finansów. Stosuj zasadę: jedno hasło = jedna strona/portal
- ✓ Chroń swoje hasła i dane do logowania– nie udostępniaj ich na portalach społecznościowych, nie rób zdjęć utworzonych haseł telefonem komórkowym.
- ✓ Nie używaj opcji automatycznego zapisywania haseł oferowanych przez portale.
- ✓ Zawsze po skończonej pracy wyloguj się ze swojego konta bankowego, z poczty e-mail, social mediów i innych używanych portali.

4.BEZPIECZNE E-ZAKUPY

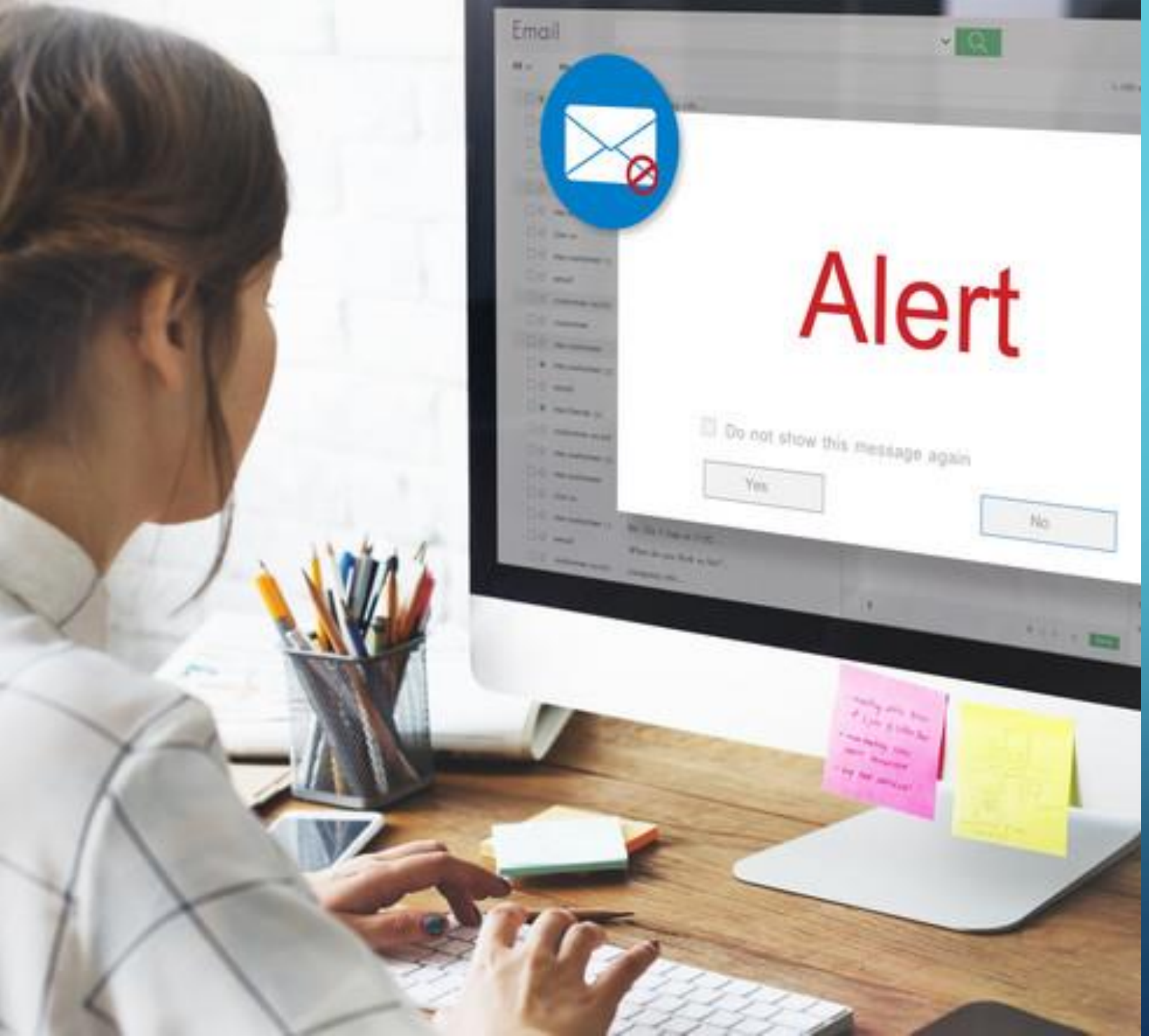
- ✓ **Używaj różnych haseł do zakładania kont w e-sklepach,** które są skomplikowane do zapamiętania i składają się z różnych znaków, mają dwuetapowe uwierzytelnianie lub używaj tokena.
- ✓ **Korzystaj z bezpiecznych metod płatności –** im więcej metod płatności (np. przelew, BLIK, PayPal, PayU, Przelewy24), oferuje dany sklep internetowy, tym większe można mieć do niego zaufanie
- ✓ **Osobna karta płatnicza lub kredytowa do zakupów online –** dokonując zakupów w sieci, musisz podać czasem dane karty (numer, datę ważności i kod CVV). Warto posiadać osobne konto lub kartę, która będzie służyła wyłącznie do zakupów online.
- ✓ **Zawsze zachowuj maile od sprzedawcy, a po otrzymaniu przesyłki paragon –** obecnie w większości sklepów po dokonaniu zakupów otrzymujesz kilka e-maili. Zawierają informację na temat tego, że właśnie dokonałeś zakupu, że wykonałeś już płatność, że wybrane przedmioty czekają na wysyłkę, zostały wysłane, będą u Ciebie wkrótce itp. Nie usuwaj tych e-maili do momentu, kiedy nie otrzymasz przesyłki – w razie pojawienia się problemów będziesz miał dowód. Po otrzymaniu paczki zachowaj paragon – w przeciwnym wypadku nie będziesz mógł zwrócić lub reklamować produktu.
- ✓ **Sprawdź sklep przed zakupem.** Wiarygodne e-sklepy zamieszczają na swoich stronach dane potwierdzające prowadzenie działalności gospodarczej (REGON, NIP, KRS, numer kontaktowy, adres siedziby). W przypadku, gdy nadal nie jesteśmy pewni co do wiarygodności strony, możemy za pomocą tych danych ją sprawdzić w oficjalnych rejestrach.

Uważaj na oszustów.

Od pewnego czasu prawdziwą plagą zakupów online są e-maile, sms pochodzące rzekomo od firm kurierskich.

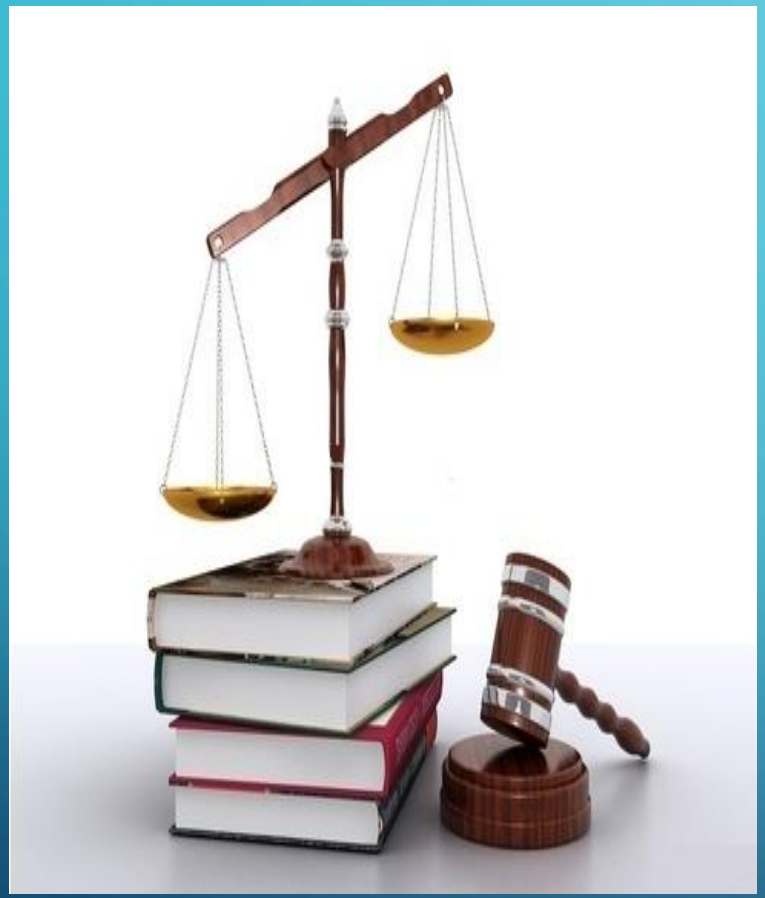
Wystarczy kliknąć w link lub pobrać załącznik, który jak się później okazuje zawierał niebezpieczne treści lub wirusa.

Internetowi przestępcy idą również o krok dalej, przesyłają wiadomości SMS z informacją, że musisz dopłacić jeszcze 20 groszy, aby przesyłka mogła do Ciebie dotrzeć – przestępcy tłumaczą np., że opłatna musi być pobrana, ponieważ przekroczona została waga paczki-co oczywiście nie jest prawdą.



5. STRACIŁEM DANE LUB DOSTĘP DO KONTA … CO ZROBIĆ?

1. **Oceń zagrożenie** (utraciłeś dostęp, bo zapomniałeś nowego hasła- czy utraciłeś dostęp, bo podejrzewasz, że ktoś włamał się na Twoje konto).
2. **Jeśli jeszcze możesz- zmień wszystkie hasła dostępu na wszystkich używanych przez siebie stronach- portalach, włącz uwierzytelnianie dwuskładnikowe- zrób to najlepiej z innego komputera.**
3. **Zweryfikuj czy ktoś jest obecnie zalogowany na Twoje konto.** Wiele serwisów pozwala na weryfikację, czy na dane konto ktoś (poza Tobą) jest obecnie zalogowany. Ta funkcja pozwala na "odłączenie" przestępcy od Twojego konta, po zmianie hasła prawdopodobnie nie będzie mógł się już ponownie zalogować.
4. **Powiadom operatora strony- portalu, że utraciłeś dostęp do konta i prosisz o pomoc.**
5. Jeśli są to portale społecznościowe- **powiadom znajomych i rodziców,** że nie jesteś autorem informacji, które mogą pojawiać się na stronie pod Twoim imieniem, nazwiskiem lub „nikiem" (pseudonimem).
6. **Powiadom bank,** jeśli podczas transakcji online ukradziono Tobie także pieniądze z konta bankowego.
7. **Powiadom policję.**
8. **Wyciągnij wnioski.**



CZY PRZESTĘPCA PONIESIE KARĘ?

Przestępstwa przeciwko ochronie informacji reguluje **Ustawa Kodeks Karny.**

Działania o charakterze przestępczym podlegają karze:

- ✓ grzywny,
- ✓ karze ograniczenia wolności,
- ✓ karze pozbawienia wolności od 3 miesięcy do 8 lat.

Zapamiętaj:

1. Korzystaj z bezpiecznych stron www.
2. Korzystaj z bezpiecznej sieci.
3. Utwórz silne hasło.
4. Jedno hasło do jednego konta w sieci.
5. Nie rób zdjęć telefonem komórkowym utworzonego hasła i nie udostępniaj go na portalach społecznościowych ani znajomym.
6. Dbaj o prywatność w sieci- tylko prawdziwi znajomi.
7. Korzystaj z bezpiecznych metod płatności.
8. Używaj osobnej karty płatniczej do zakupów online.
9. Zawsze zachowuj maile od sprzedawcy, a po otrzymaniu przesyłki paragon.
10. Zawsze po skończonej pracy wyloguj się ze swojego konta.

TY odpowiadasz za swoje bezpieczeństwo w sieci ☺

DZIEŃ BEZPIECZNEGO INTERNETU 2021

Uczymy się od siebie dla siebie.

Opracowanie materiałów:

Sandra Czechowicz, kl.2CE – Technik Ekonomista

Aleks Malinowski, kl.2BH- Technik Handlowiec