Link od „znajomego” – warto wiedzieć zanim klikniesz!

Link od „znajomego” – warto wiedzieć zanim klikniesz!

W związku z trwającą pandemią i licznymi ograniczeniami w korzystaniu z ulubionych miejsc rozrywki takich jak kina, teatry, czy kawiarnie i restauracje, a także ograniczeniem naszych kontaktów towarzyskich, coraz więcej czasu poświęcamy na rozrywkę w Internecie i za jego pośrednictwem kontaktujemy się również ze znajomymi. Co może nam wtedy grozić i jak tych zagrożeń uniknąć, dowiesz się z poniższego artykułu.

Mail od „znajomego”

Za oknem pada deszcz, w telewizji znów powtórka kultowej komedii, którą znasz już na pamięć…Jak umilić sobie czas? Może warto poszperać po Internecie lub sprawdzić zaległą pocztę e-mail? Uruchamiamy więc komputer, otwieramy pocztę, a tu niespodzianka – wiadomość mailowa od znajomego, z którym dawno nie mieliśmy kontaktu! Czytamy więc pospiesznie maila, żeby dowiedzieć się, co u niego słychać. Treść maila jest jednak dość skąpa i ogranicza się do przesłania linku z poleceniem świetnego spektaklu, który można obejrzeć w Internecie. Trochę dziwny ten mail, ponieważ po długiej przerwie w kontaktach spodziewalibyśmy się czegoś więcej, ale może warto kliknąć?

Nie daj się złapać na phisha

Phishing to powszechne działanie oszustów internetowych, polegające na próbie wyłudzenia naszych wrażliwych danych przy wykorzystaniu zabiegów socjotechnicznych, czyli mówiąc potocznie manipulacji.

Oszuści mogą podszywać się pod naszych znajomych lub znane nam i budzące nasze zaufanie instytucje, aby nakłonić nas do kliknięcia w złośliwy link lub otwarcia złośliwego załącznika. Co to jest złośliwy link? To link prowadzący na przykład do fałszywej strony internetowej z usługą rejestracji lub logowania, która przechwytuje dane po ich wprowadzeniu. Link może też spowodować zainfekowanie komputera i zainstalowanie na nim złośliwego oprogramowania, które będzie śledzić nasze działania w sieci i w efekcie również do przechwycenia wprowadzanych przez nas wrażliwych danych, takich jak numer PESEL, seria i nr dowodu tożsamości, dane logowania do bankowości internetowej.

Jak się bronić przed phishingiem

Odbierając maila od „znajomego” otrzymaliśmy też sygnały świadczące o tym, że mail może być fałszywy. Przecież znajomy dawno się do nas nie odzywał i nagle bez słowa wstępu i wyjaśnienia przesyła nam link do strony ze spektaklem? Każda taka niestandardowa sytuacja powinna wzbudzić nasze podejrzenia.

Adres nadawcy

Warto więc sprawdzić, czy jest to na pewno mail od naszego znajomego, sprawdzając dokładnie adres mailowy – czy nie różni się nieznacznie od prawdziwego adresu, z którego zawsze otrzymywaliśmy od niego maile, np. kropką pomiędzy imieniem i nazwiskiem, czy też zastosowaniem podobnych liter np. „r” i „n”, które obok siebie wyglądają jak „m”. Aby to sprawdzić można skopiować adres nadawcy do dokumentu Word i powiększyć czcionkę.

Zawis kursora

Co jednak, jeśli mail wydaje się wiarygodny i mamy ogromną ochotę obejrzeć ciekawy spektakl? W takiej sytuacji warto dokładnie sprawdzić link. W tym celu najlepiej wykonać tzw. zawis kursora, a więc najechać kursorem na link, nie klikając jednak w niego! Pokaże nam się wtedy prawdziwy adres, do którego link nas odsyła – niekoniecznie taki sam, jak ten widoczny w mailu.

Co zrobić, gdy rozpoznamy phishing?

Jeśli więc nadesłany e-mail budzi nasze podejrzenia i potwierdzą się one po sprawdzeniu adresu nadawcy oraz linku powinniśmy zrobić tylko jedno – usunąć maila. Nie należy przesyłać maila do znajomych, aby podzielić się wrażeniami czy poprosić ich o sprawdzenie go, gdyż narażamy ich wtedy na niebezpieczeństwo. Pamiętajmy także, że złośliwy link możemy otrzymać nie tylko w mailu, ale również w wiadomości sms. Mamy wtedy do czynienia z tzw. smishingiem.

PAMIĘTAJ!

- Jeśli treść maila lub okoliczności w jakich go otrzymałeś budzą Twoje wątpliwości zachowaj czujność i sprawdź go dokładnie
- Sprawdź, czy adres nadawcy jest prawdziwy i nie ma literówek lub znaków specjalnych wewnątrz adresu
- Nigdy nie klikaj w linki otrzymane w mailu bez sprawdzenia ich, a najlepiej wejdź bezpośrednio na stronę instytucji, z której usługi chcesz skorzystać i sprawdź czy oferuje to, o czym była mowa w mailu.
- W razie wątpliwości lub obaw, zwróć się do osoby, do której masz zaufanie i która ma większą wiedzę na temat zagrożeń w sieci i opowiedz jej o zdarzeniu.

BĄDŹ CZUJNY!

Program sektorowy „Bankowcy dla Edukacji" to jeden z największych programów edukacji finansowej w Europie. Jest on realizowany od 2016 r. z inicjatywy Związku Banków Polskich przez Warszawski Instytut Bankowości. Jego celem jest edukowanie uczniów, studentów i seniorów w zakresie podstaw praktycznej wiedzy dotyczącej ekonomii, finansów, bankowości, przedsiębiorczości, cyberbezpieczeństwa i obrotu bezgotówkowego.

Dowiedz się więcej na **www.bde.wib.org.pl**