Co-funded by the European Union

Zagrożenia online dla osób 55+ – słownik

Co-funded by the
European Union

Phishing (oszukańcze wiadomości e-mail, SMS-y, linki, połączenia głosowe)

Phishing to rodzaj cyberataku, w którym przestępcy wysyłają fałszywe e-maile, SMS-y, połączenia telefoniczne lub linki, podszywając się pod kogoś, komu ufasz, np. bank lub znajomego. Ich celem jest nakłonienie Cię do podania ważnych danych osobowych, takich jak hasła, numery kart kredytowych lub dane konta bankowego. Te fałszywe wiadomości często wyglądają bardzo realistycznie i próbują nakłonić Cię do szybkiego działania, wywołując poczucie pilności lub strachu. Atakujący chcą ukraść Twoje pieniądze lub tożsamość, nakłaniając Cię do kliknięcia w niebezpieczne linki lub udostępnienia poufnych danych. Aby zachować bezpieczeństwo, zawsze dokładnie sprawdzaj, kto jest nadawcą wiadomości, unikaj klikania w podejrzane linki i nigdy nie udostępniaj danych osobowych, jeśli nie masz absolutnej pewności, że są bezpieczne.

Co-funded by the
European Union

Ataki deepfake (fałszywe materiały audio/wideo, podszywanie się pod członków rodziny)

Ataki deepfake polegają na tworzeniu fałszywych nagrań audio lub wideo za pomocą sztucznej inteligencji, które wyglądają i brzmią bardzo realistycznie. W tych atakach przestępcy imitują głos lub twarz znanej osoby, często członka rodziny, aby wmówić rozmówcy, że rozmawiają z bliską osobą. Na przykład, oszust może użyć technologii deepfake, aby wykonać połączenie telefoniczne, które brzmi dokładnie jak wnuczka prosząca o pilne pieniądze. Te fałszywe nagrania są bardzo przekonujące i mogą oszukać nawet ostrożne osoby. Ataki deepfake są niebezpieczne, ponieważ wykorzystują zaufanie i emocje, utrudniając rozpoznanie oszustwa, dopóki nie jest za późno. Aby się chronić, zawsze weryfikuj nietypowe prośby, kontaktując się z daną osobą bezpośrednio za pośrednictwem różnych kanałów komunikacji, zanim podejmiesz jakiekolwiek działania.

Co-funded by the
European Union

Fałszywe sklepy internetowe i oszustwa (fałszywe strony internetowe)

Fałszywe sklepy internetowe i oszustwa to fałszywe strony internetowe, które wyglądają jak legalne sklepy, ale w rzeczywistości służą do nakłaniania ludzi do zakupu produktów, które nie istnieją lub są niskiej jakości. Te fałszywe sklepy często kopiują logo, opisy produktów i zdjęcia prawdziwych firm, aby wyglądać przekonująco. Oszuści wykorzystują te strony do kradzieży pieniędzy i danych osobowych niczego niepodejrzewających klientów. Wabią kupujących obietnicami bardzo niskich cen lub ofert specjalnych, które wydają się zbyt piękne, aby mogły być prawdziwe.

Te strony internetowe mogą mieć dziwne adresy internetowe, zawierać błędy ortograficzne lub brakować prawidłowych danych kontaktowych. Po dokonaniu płatności klienci często nie otrzymują zamówienia lub otrzymują podróbki. Aby się chronić, zawsze kupuj w zaufanych sklepach, sprawdzaj opinie o stronach, unikaj ofert, które wydają się nierealistycznie tanie i nigdy nie udostępniaj danych do płatności na podejrzanych stronach. Jeśli coś wydaje Ci się podejrzane, lepiej to sprawdzić przed zakupem.

Co-funded by the
European Union

Manipulacja emocjonalna i inżynieria społeczna (taktyka zastraszania)

Manipulacja emocjonalna i socjotechnika polegają na oszukiwaniu ludzi poprzez grę na ich emocjach, aby skłonić ich do działania w sposób, którego normalnie by nie zrobili. Cyberprzestępcy stosują taktyki takie jak straszenie, natarczywość, udawanie autorytetu lub życzliwości, aby wywołać poczucie strachu, zaufania lub obowiązku. Na przykład mogą udawać pracownika banku ostrzegającego o problemie z kontem, nakłaniając do szybkiego działania, aby bez zastanowienia podać poufne informacje. Taktyki te wykorzystują naturalne ludzkie reakcje – strach, zaufanie, ciekawość lub chęć pomocy – utrudniając im opór. Najlepszą obroną jest świadomość: rozpoznanie tych emocjonalnych sztuczek i zatrzymanie się, aby zweryfikować, kto naprawdę prosi o informacje, zanim odpowie.

Co-funded by the
European Union

Kradzież tożsamości (wykorzystując skradzione dane osobowe)

Kradzież tożsamości oznacza sytuację, gdy ktoś kradnie Twoje dane osobowe bez Twojej zgody i wykorzystuje je, podszywając się pod Ciebie. Może wykorzystać Twoje imię i nazwisko, numer ubezpieczenia społecznego, dane konta bankowego lub inne dane do zakładania kont, zaciągania pożyczek lub dokonywania zakupów w Twoim imieniu. Może to spowodować poważne problemy finansowe i zaszkodzić Twojej reputacji.

Co-funded by the
European Union

Oszustwo „na wnuka” (oszuści podszywający się pod rodzinę w tarapatach)

Oszustwo „na wnuka”, znane również jako „oszustwo na dziadka”, to powszechna metoda stosowana przez przestępców, którzy podszywają się pod członka rodziny – zazwyczaj wnuka lub dziecko – w potrzebie. Zazwyczaj odbywa się to telefonicznie, kiedy oszust dzwoni do osoby starszej i twierdzi, że ma poważne kłopoty, takie jak wypadek, została aresztowana lub potrzebuje pilnej pomocy finansowej. Dzwoniący często prosi o szybkie przesłanie pieniędzy i nalega, aby ofiara zachowała to w tajemnicy, na przykład mówiąc: „Nie mów mamie, bo się zmartwi”.

To oszustwo wykorzystuje emocje, takie jak miłość i troska o członków rodziny, sprawiając, że osoba chce natychmiast pomóc, bez chwili namysłu. Coraz częściej oszuści wykorzystują technologie takie jak sztuczna inteligencja, aby naśladować głos prawdziwego wnuka, dzięki czemu rozmowa brzmi bardzo przekonująco.

Co-funded by the
European Union

Fałszywe prośby o „pomoc” przez WhatsApp lub Messenger

Fałszywe prośby o „pomoc” za pośrednictwem WhatsApp lub Messengera to oszustwa, w których ktoś podszywa się pod znajomego lub członka rodziny w pilnych tarapatach, prosząc o pieniądze lub dane osobowe. Wiadomości te często przychodzą niespodziewanie od nieznanych lub podszywających się osób. Oszust może twierdzić, że zgubił telefon, został zablokowany na koncie lub potrzebuje pilnej pomocy finansowej. Stara się stworzyć poczucie pilności i zaufania, aby skłonić ofiary do szybkiego działania, nie sprawdzając, czy to prawda.

Co-funded by the
European Union

Oszustwa matrymonialne i oszustwa oparte na związkach budowanych w Internecie

Oszustwa matrymonialne to rodzaj oszustwa, w którym przestępcy tworzą fałszywe profile internetowe i udają zainteresowanie daną osobą. Z czasem budują zaufanie i więź emocjonalną, wmawiając ofierze, że jest w prawdziwym związku. Po zdobyciu zaufania, oszuści wymyślają nagłe przypadki lub pilne potrzeby finansowe – takie jak rachunki za leczenie czy koszty podróży – i proszą ofiarę o pieniądze lub prezenty.

Ci oszuści potrafią doskonale udawać troskliwych i godnych zaufania, często unikając spotkań osobistych lub rozmów wideo, podając wymówki. Wykorzystują samotność i emocjonalną wrażliwość ofiar, co zwiększa prawdopodobieństwo, że dadzą im pieniądze.

Co-funded by the
European Union

Oszustwa inwestycyjne (fałszywe reklamy z udziałem gwiazd)

Oszustwa inwestycyjne z wykorzystaniem fałszywych reklam z udziałem celebrytów to rodzaj oszustwa, w którym przestępcy wykorzystują zdjęcia, filmy lub nazwiska znanych osób, aby przedstawić okazję inwestycyjną jako legalną i wiarygodną. Czasami reklamy te zawierają filmy deepfake, na których celebryci rekomendują daną inwestycję, lub podszywają się pod artykuły prasowe, łączące celebrytów z sukcesami finansowymi na określonych platformach.

Oszuści wmawiają ludziom, że mogą szybko i dużo zarobić, często w kryptowalutach lub handlu walutami. Nakłaniają ofiary do zakładania kont, wpłacania pieniędzy, a następnie proszą o dodatkowe środki na pokrycie fałszywych opłat lub podatków. Szybkie zwroty mogą okazać się sposobem na zdobycie zaufania, ale gdy ofiary próbują wypłacić pieniądze, zostają zablokowane i poproszone o dodatkowe, wysokie płatności.

Co-funded by the
European Union

Oprogramowanie złośliwe i ransomware (zainfekowane pliki, załączniki)

Złośliwe oprogramowanie (malware) to złośliwe oprogramowanie, które może zainfekować komputer lub telefon i spowodować szkody, takie jak kradzież danych osobowych, uszkodzenie plików lub przejęcie kontroli nad urządzeniem. Ransomware to specjalny rodzaj złośliwego oprogramowania, który blokuje lub szyfruje pliki, uniemożliwiając dostęp do nich do momentu zapłacenia atakującemu okupu – zazwyczaj w kryptowalucie. Ransomware może przedostać się na urządzenie za pośrednictwem zainfekowanych załączników do wiadomości e-mail, złośliwych stron internetowych lub niebezpiecznych plików do pobrania.

Po zainfekowaniu ransomware uniemożliwia korzystanie z ważnych plików, a czasami żąda pieniędzy za przywrócenie dostępu. Zapłacenie okupu nie gwarantuje uwolnienia danych, a wręcz zachęca przestępców do kontynuowania ataków.

Co-funded by the
European Union

Niezweryfikowane aplikacje i pobieranie niebezpiecznego oprogramowania

Niezweryfikowane aplikacje i niebezpieczne pobieranie oprogramowania to cyberzagrożenia, które polegają na pobieraniu i instalowaniu aplikacji lub plików z nieznanych lub niepewnych źródeł. Te aplikacje lub pliki mogą zawierać ukryte złośliwe oprogramowanie, wirusy lub oprogramowanie szpiegujące, które może uszkodzić urządzenie, wykraść dane osobowe lub umożliwić hakerom nieautoryzowany dostęp.

Ponieważ te aplikacje nie są sprawdzane ani zatwierdzane przez zaufane platformy, mogą one zakłócać bezpieczeństwo Twojego urządzenia, powodować awarie lub narażać Cię na oszustwa. Fałszywe aplikacje mogą wyglądać jak prawdziwe, ale po zainstalowaniu mogą gromadzić Twoje dane lub rozprzestrzeniać szkodliwe oprogramowanie.

Co-funded by the
European Union

Udostępnianie wrażliwych danych obcym osobom (zdjęć, informacji)

Udostępnianie poufnych danych, takich jak zdjęcia czy dane osobowe, obcym osobom to cyberzagrożenie, polegające na udostępnianiu prywatnych danych nieznanym lub niegodnym zaufania osobom w sieci. Może się to wydawać nieszkodliwe, jak udostępnianie zdjęcia, ale dane te mogą zostać wykorzystane do kradzieży tożsamości, popełnienia oszustwa lub zaszkodzenia reputacji.

Zdjęcia mogą ujawnić Twój dom, lokalizację lub nawyki osobiste, nawet jeśli tego nie zauważysz. Nieznajomi mogą wykorzystać te informacje, aby Cię oszukać lub wykorzystać do oszustw. Aby zachować bezpieczeństwo, udostępniaj dane osobowe i zdjęcia tylko osobom, którym ufasz, zastanów się dobrze, zanim opublikujesz je w internecie, i dostosuj ustawienia prywatności, aby ograniczyć liczbę osób, które mogą zobaczyć Twoje dane.

Co-funded by the
European Union

Wycieki danych z powodu korzystania z przestarzałych urządzenia lub oprogramowanie

Korzystanie z przestarzałych urządzeń lub oprogramowania stanowi cyberzagrożenie, ponieważ stare wersje często nie posiadają najnowszych aktualizacji zabezpieczeń. Brak aktualizacji tworzy słabe punkty, zwane lukami, które hakerzy mogą łatwo wykorzystać do uzyskania dostępu do danych osobowych lub przejęcia kontroli nad urządzeniem. Może to prowadzić do wycieku danych, kradzieży lub infekcji złośliwym oprogramowaniem.

Przestarzałe oprogramowanie również spowalnia działanie urządzenia i może przestać działać z nowszymi programami, utrudniając codzienne czynności. Aby się chronić, ważne jest regularne aktualizowanie urządzenia i oprogramowania najnowszymi poprawkami i poprawkami bezpieczeństwa. Pozwala to wyeliminować luki w zabezpieczeniach, zapewnić bezpieczeństwo danych i płynne działanie urządzenia.

Co-funded by the
European Union

Masowe, spersonalizowane ataki wykorzystujące sztuczną inteligencję, mające na celu profile użytkowników

Masowe ataki personalizowane z wykorzystaniem sztucznej inteligencji to cyberzagrożenia, w których atakujący wykorzystują sztuczną inteligencję do tworzenia wysoce spersonalizowanych i przekonujących komunikatów skierowanych do konkretnych osób w oparciu o ich dane osobowe. Sztuczna inteligencja analizuje informacje z mediów społecznościowych, wiadomości e-mail i źródeł publicznych, aby tworzyć komunikaty, które wydają się znajome i godne zaufania dla ofiary.

Ataki te mogą obejmować spersonalizowane e-maile lub wiadomości phishingowe, które zawierają imię i nazwisko ofiary, jej zawód, ostatnie aktywności lub zainteresowania. Celem jest nakłonienie użytkowników do kliknięcia w złośliwe linki, ujawnienia haseł lub przelania pieniędzy. Ponieważ sztuczna inteligencja stale się uczy i adaptuje, ataki te stają się skuteczniejsze i trudniejsze do wykrycia.

Co-funded by the
European Union

Dezinformacja zdrowotna lub niebezpieczne porady medyczne pochodzące z narzędzi AI

Dezinformacja zdrowotna lub niebezpieczne porady medyczne pochodzące z narzędzi AI to cyberzagrożenie, w którym sztuczna inteligencja generuje nieprawidłowe, wprowadzające w błąd lub szkodliwe informacje zdrowotne. Ludzie mogą ufać chatbotom AI lub narzędziom online w zakresie porad medycznych, ale czasami systemy te stawiają błędne diagnozy, sugerują niebezpieczne metody leczenia lub rozpowszechniają fałszywe informacje na temat chorób.

Ta dezinformacja może prowadzić do opóźniania odpowiedniej opieki medycznej, stosowania nieskutecznych metod leczenia lub podejmowania szkodliwych działań. Treści generowane przez sztuczną inteligencję mogą brzmieć bardzo profesjonalnie i przekonująco, przez co trudno ocenić, czy porady są wiarygodne.

Co-funded by the
European Union

Oszustwa wykorzystujące wykluczenie cyfrowe w służbach obywatelskich i bankowych

Oszustwa wykorzystujące wykluczenie cyfrowe w usługach obywatelskich i bankowych to zagrożenia skierowane do osób z ograniczonym dostępem do technologii cyfrowych lub ich ograniczoną znajomością. Oszustwa te wykorzystują osoby, które mają trudności z korzystaniem z internetowych usług rządowych lub bankowych, czasami z powodu braku urządzeń, dostępu do internetu, umiejętności cyfrowych lub pewności siebie.

Przestępcy oszukują te osoby, oferując fałszywą pomoc w procesach online lub wysyłając fałszywe wiadomości podszywające się pod oficjalne instytucje, licząc na to, że ofiary udostępnią poufne dane lub prześlą pieniądze. Ponieważ osoby te mają mniej zasobów lub wsparcia, aby rozpoznać oszustwa, są bardziej podatne na ataki.

Co-funded by the
European Union

Brak praktyk uwierzytelniania wieloskładnikowego (uproszczone hasła, ponowne wykorzystanie)

Brak uwierzytelniania wieloskładnikowego (MFA) oznacza używanie wyłącznie hasła – często prostego lub powtarzanego na wielu stronach – do ochrony kont online. Jest to ryzykowne, ponieważ jeśli ktoś ukradnie lub odgadnie Twoje hasło, może łatwo uzyskać dostęp do Twoich kont.

Uwierzytelnianie wieloskładnikowe dodaje dodatkową warstwę bezpieczeństwa, wymagając dwóch lub więcej form weryfikacji. Na przykład, po wpisaniu hasła, możesz wpisać kod wysłany na telefon lub skorzystać ze skanu odcisku palca. To znacznie utrudnia hakerom dostęp do Twojego konta, nawet jeśli znają Twoje hasło.

Co-funded by the
European Union

Utrata dostępu do kluczowych usług z powodu zmian technologicznych (dostęp tylko za pośrednictwem aplikacji, ograniczone alternatywy)

Utrata dostępu do kluczowych usług spowodowana zmianami technologicznymi ma miejsce, gdy ważne usługi publiczne lub bankowe przechodzą na formaty wyłącznie cyfrowe, takie jak aplikacje czy portale internetowe, bez łatwych alternatyw dla osób, które nie czują się komfortowo lub nie mają do nich dostępu. Oznacza to, że osoby nieposiadające smartfonów, komputerów ani umiejętności cyfrowych mogą mieć trudności lub wręcz nie mieć dostępu do podstawowych usług, takich jak wizyty u lekarza, świadczenia emerytalne czy transakcje bankowe.

Ta cyfrowa zmiana może powodować wykluczenie wielu osób, zwłaszcza starszych i tych o ograniczonych zasobach, czyniąc je zależnymi od innych lub uniemożliwiając im realizację ważnych zadań.

Co-funded by the
European Union

Zautomatyzowana manipulacja kanałami mediów społecznościowych, powodująca dezinformację i stres

Zautomatyzowana manipulacja kanałami mediów społecznościowych to cyberzagrożenie, w którym programy komputerowe, zwane botami, oraz sztuczna inteligencja kontrolują treści, które widzisz na swoich stronach w mediach społecznościowych. Systemy te analizują, co lubisz, udostępniasz lub komentujesz, a następnie wyświetlają Ci więcej podobnych postów, aby utrzymać Twoje zaangażowanie.

Niestety, może to być wykorzystywane do rozpowszechniania dezinformacji, fałszywych wiadomości lub treści ekstremalnych, wywołujących stres, strach lub gniew. Boty mogą sztucznie zwiększać popularność takich postów poprzez lajkowanie, udostępnianie lub komentowanie, sprawiając wrażenie, że wiele osób się z nimi zgadza.