Odcinek 2: Jak działają cyberoszuści i jak się przed nimi chronić?

Transkrypcja wideo edukacyjnego dla seniorek i seniorów

Wyjaśnia dr Marlena Kondrat, doktor nauk społecznych w dyscyplinie ekonomia i finanse, Uniwersytet Warszawski, Uniwersytet Civitas

Kompetencje cyfrowe seniorów w Polsce

W Polsce mamy zaledwie 13% osób w wieku 65–74 lata, które posiadają podstawowe umiejętności cyfrowe. Niestety średnia unijna wynosi około 30%, więc jesteśmy na szarym końcu. I co rozumiemy właściwie poprzez umiejętności cyfrowe, podstawowe umiejętności? Mówimy tutaj o prostym wyszukiwaniu informacji w internecie, weryfikacji różnych źródeł, co bardzo ważne dla osób starszych, również komunikacji poprzez znane komunikatory z bliskimi, z rodziną, ze znajomymi. Są to bardzo ważne kompetencje, bez których obecnie ciężko jest nam poruszać się w takim scyfryzowanym świecie, gdzie chociażby idąc do apteki, powinniśmy zrealizować e-receptę, zrealizować proste płatności finansowe czy zeskanować kod QR. Bez takich umiejętności, niezależnie od wieku, jest nam bardzo ciężko poruszać się w takiej rzeczywistości.

Zagrożenie technologią deepfake

Podczas rozmów z seniorami bardzo często spotykamy się z informacją, że zwłaszcza w mediach społecznościowych stykają się z deepfake'ami. Czyli właśnie widzą, że rzekomo prezydent przedstawił jakiś bardzo ważny komunikat, oczywiście związany z zagrożeniem. To sprzyja dezinformacji. To sieje zamęt wśród różnych osób, niezależnie od wieku. Dlatego bardzo ciężko jest rozpoznać, co jest prawdą, a co nie, zwłaszcza dla osób, które nie są zaznajomione z tym nowym światem, gdzie sztuczna inteligencja wykorzystywana jest w bardzo, bardzo wyrafinowany sposób do tego, aby oszukiwać. Seniorzy potrzebują jasnych przykładów. Jeżeli mówimy „deepfake", to co przez to rozumiemy? Mówimy prostym językiem, że to są często sfałszowane komunikaty, które rzekomo wypowiada osoba będąca autorytetem, na przykład prezydent, osoba pełniąca wysokie funkcje publiczne. Osoby starsze mają bardzo duży problem z rozróżnieniem i weryfikowaniem, czy rzeczywiście ta osoba była w stanie wypowiedzieć takie słowa, czy też nie.

Mechanizmy manipulacji i weryfikacja źródeł

Mówimy tutaj już o bardzo zaawansowanych metodach z wykorzystaniem sztucznej inteligencji, więc jest to podkładanie tekstu do danej osoby, dostosowanie ruchu ust do tej osoby tak, żeby wyglądało to maksymalnie rzeczywiście. W sytuacji, kiedy widzimy, że dany komunikat brzmi bardzo niepokojąco, że nie do końca może być to zbieżne z prawdą, warto jest szukać informacji już nie w mediach społecznościowych, ale właśnie poprzez przeglądarkę dotrzeć do wiarygodnych źródeł. W sytuacji, kiedy spotkamy się z informacją w mediach społecznościowych, która budzi w nas niepokój i nie do końca jesteśmy przekonani, czy jest zgodna z prawdą, warto skorzystać ze źródeł bardziej wiarygodnych, czyli wychodzimy z mediów społecznościowych i poprzez wyszukiwarkę czy za pomocą mediów takich jak telewizja, prasa szukamy, czy rzeczywiście ma to związek z prawdą, czy niekoniecznie. Głównym celem cyberoszustów jest przekazywanie i zachęcanie do udostępniania tych nieprawdziwych informacji.

Rola emocji w dezinformacji

Podczas spotkań z seniorami na uniwersytetach III wieku bardzo często spotykałam się z informacją, że posty, które widzą właśnie na stronach internetowych, czy to nieprawdziwe informacje, czy wspomniane wcześniej deepfake'i, wywołują w nich strach. To jest ta pierwsza emocja, która sprawia, że reagują, że chcą udostępniać dalej, być może też chronić swoich bliskich. Dlatego powinniśmy pamiętać, że każdy komunikat, którego głównym celem jest wywoływanie strachu, powinien być przez nas kilkukrotnie sprawdzony. To jest bardzo ważne w kontekście wojny hybrydowej czy ostatnich wydarzeń, z którymi mamy bardzo często do czynienia, którym towarzyszy dezinformacja i rozsiewanie nieprawdziwych informacji po to, żeby właśnie wzbudzać niepokój. Jest to ta pierwsza emocja, na której bazują oszuści.

Metody ochrony i zgłaszanie przestępstw

Czym natomiast warto się dzielić? Możemy podzielić się w internecie informacjami czy też naszymi osiągnięciami z zakresu szkoleń, pokazać, że istnieją odpowiednie miejsca, w których taką wiedzę możemy zdobyć. Podzielić się właśnie z bliskimi, pokazać, gdzie mogą zdobyć taką wiedzę, gdzie mogą poczuć się bezpieczni dzięki temu, że dostosowują się do nowych realiów. Co możemy zrobić, aby chronić siebie w internecie? Możemy wykorzystywać technologie w tym celu poprzez:

1. Instalację oprogramowania antywirusowego.
2. Korzystanie z aplikacji bankowych, które są zdecydowanie bezpieczniejsze niż korzystanie ze stron w internecie.
3. Blokowanie podejrzanych numerów telefonicznych czy też właśnie adresów e-mail.
4. I z drugiej strony to, co najważniejsze – zgłaszanie cyberprzestępstwa.

Pamiętajmy, że w ten sposób chronimy nie tylko siebie, ale również naszych bliskich. Bo im częściej zgłaszamy, tym bardziej organy odpowiedzialne za sprawdzanie cyberprzestępstw chronią nas skuteczniej, tworzą nowe rozwiązania i nowe ścieżki do tego, abyśmy mogli czuć się bezpieczniej w tym nowym cyfrowym świecie.

Znaczenie edukacji dla społeczeństwa

Nowe technologie rozwijają się na niespotykaną dotąd skalę, dlatego musimy być świadomi nowych cyberoszustw, z którymi będziemy mieć do czynienia zarówno w przestrzeni cyfrowej, jak i w świecie rzeczywistym. Podsumowując, inwestycja w edukację cyfrową osób starszych to inwestycja w niezależność i lepszą jakość życia całego społeczeństwa. Dlatego bardzo ważne jest, abyśmy skupiali się na wszystkich grupach społecznych, bo to oznacza z jednej strony lepszą jakość życia, z drugiej strony seniorzy będą też bardziej świadomymi konsumentami, a to przekłada się też na lepszą działalność ze strony instytucji i rządu, którzy mają mniej takich zgłoszeń oraz incydentów, a zarazem lepiej funkcjonuje się całemu społeczeństwu.

Ministerstwo Finansów
FUNDUSZ EDUKACJI FINANSOWEJ
think!
FUNDACJA ROZWOJU SPOŁECZEŃSTWA WIEDZY

Sfinansowano ze środków Funduszu Edukacji Finansowej, którego dysponentem jest Minister Finansów i Gospodarki. Realizatorem Kampanii jest Fundacja Think!