Haki na cyberataki

Bezpieczne Fin@nse

cz. 5 Bezpieczne korzystanie z płatności za zakupy w Internecie

Słowo wstępu

Starzenie się społeczeństwa jest obecnie procesem uznawanym za powszechny trend w krajach Europy Zachodniej. Społeczne transformacje przynoszą jakościowe zmiany w sposobie definiowania wykluczenia społecznego. Konsekwencje starzenia się społeczeństwa niosą wiele obaw o przyszłość krajów europejskich, w tym także Polski.

Współczesna rzeczywistość ulega szybkim przeobrażeniom w wielu obszarach. Umiejętność przystosowywania się do zachodzących zmian nabiera cywilizacyjnego wymiaru. Na szczególną uwagę zasługuje gwałtowny postęp technologiczny i rozwój rynku nowych technologii, zwłaszcza informacyjno-komunikacyjnych. Współczesne systemy społeczno gospodarcze społeczeństwa, a także państwa są uzależnione od technologii.

Umiejętność bezpiecznego korzystania z nowych technologii informacyjno-komunikacyjnych staje się koniecznością, a jej brak skutkuje ostracyzmem , społecznym wykluczeniem, narażeniem na ataki, które kończą się utratą środków. Internet a także rozwój aplikacji jest najtrudniejszy do zaakceptowania i czynnego używania jest przez seniorów. Wynika to z mniejszego tempa przyswajania wiedzy, ale też ostracyzmu tej grupy społecznej. Senior to tak ze łatwy punkt ataku.

Całość składa się z 6 cykli, które zostaną finalnie opublikowane jako jeden podręcznik pt. Bezpieczne Fin@nse. Kolejne części będą się pojawiały w odstępie 3 tygodni, wraz z filmem wprowadzającym do zagadnienia, które będą dostępne m.in. na stronie fundacji Pro Economico Bono, oraz jej mediach społecznościowych (Facebook, You Tube).

1) Bezpieczne korzystanie z e-bankowości
2) Bezpieczne korzystanie z m-bankowości
3) Bezpieczne korzystanie z karty kredytowej i debetowej (płatności w sklepie i wypłata z bankomatu)
4) Bezpieczne korzystanie z social media (komunikatory What's App podawanie danych newralgicznych)
5) Bezpieczne korzystanie z płatności za zakupy w Internecie
6) Atak ceberprzestępczy co zrobić?

Dzięki poradnikowi osoby starsze:

1. zwiększą wiarę w otworzenie i własne możliwości związane z bezpiecznym
2. korzystaniem z nowych technologii
3. zwiększą samoocenę w aspekcie technologiczno-komunikacyjnym
4. zwiększą motywację do bezpiecznego korzystania z nowych technologii, a zarazem oszczędności czasu
5. zmienią sposób myślenia w temacie nowych technologii i bezpieczeństwa z nimi związanych

Obecnie oddaję Państwu do czytania cz. 5 Poradnika Bezpieczne Fin@nse Bezpieczne korzystanie z płatności za zakupy w Internecie

Zapraszam do lektury i zgłębiania tematu, jakże ważnego w dzisiejszym, bardzo dynamicznym otoczeniu.

prof. ucz. dr inż. Robert Jeżewski

Prezes Zarządu Fundacji Pro Economico Bono

cz. 5 Bezpieczne korzystanie z płatności za zakupy w Internecie

1. ZAWSZE SPRAWDZAJ DANE PRZELEWU

ZAWSZE uważnie sprawdzaj wszystkie dane dotyczące przelewu tj. numeru rachunku bankowego i kwotę. Sytuacja ta dotyczy każdego systemu płatniczego PayU, PayPal, BLIK. Cyberprzestępcy często podmieniają te dane, licząc, że osoba wykonująca operację transferu środków nie zwróci na to uwagi.

2. KUPUJ TYLKO W SPRAWDZONYCH E-SKLEPACH

Kupujący często szuka towaru w dobrej cenie. I o tym wiedzą także cyberprzestępcy. Cena jest ważna, ale bezpieczeństwo zakupowe jeszcze bardziej. Dlatego ZAWSZE wybieraj sklepy, które nie budzą wątpliwości. Jeśli je masz poczytaj opinie i zweryfikuj je z rzeczywistością. Sprawdź czy są podane dane firmy, jej nr NIP, REGON, dane kontaktowe. Zweryfikuj opinie klientów. Jeśli występuje duża ilość negatywnych, zastanów się trzy razy, zanim dokonasz zakupu.

3. KORZYSTAJ TYLKO Z BEZPIECZNYCH SIECI WI-FI

NIGDY nie loguj się za pomocą publicznej sieci Wi-Fi. Rodzi to możliwość nadużyć i ingerencji w Twoje urządzenie mobilne ze strony właściciela sieci bezprzewodowej, oraz użytkowników, którzy z niej korzystają.

4. ZAWSZE SPRAWDZAJ CZY STRONA POSIADA WAŻNY PROTOKÓŁ HTTPS

Protokół HTTPS gwarantuje prywatność i bezpieczeństwo połączenia. Można go sprawdzić najeżdżając kursorem na kłódkę. Kłódka musi być zamknięta a po kliknięciu w nią można sprawdzić, czy certyfikat SSL jest ważny a także na kogo został wystawiony. Jeżeli kłódka jest otwarta i/lub certyfikat wystawiony nie na bank, ZREZYGNUJ z logowania się.

5. MONITORUJ SWOJĄ AKTYWNOŚC NA KONCIE BANKOWYM

Sprawdzaj aktywność na swoim koncie. Dzięki temu możesz wykryć czy ktoś obcy nie logował się do Twojego elektronicznego konta bankowego. Wczesne rozpoznanie może uratować Twoje finanse. W przypadku wykrycia, że ktoś inny zalogował się do Twojego konta, natychmiast zmień hasło do konta i zgłoś sprawę do banku.

6. BĄDŹ CZUJNY I UWAŻAJ NA PODEJRZANE WIADOMOŚCI E-MAIL/SMS

Zakupy internetowe to otrzymywanie sporej ilości wiadomości, np. o realizacji zlecenia, płatności, dostawie, itp. Warto uważnie się im przyglądać, z uwagi na fakt, że jest to popularna metoda wyłudzania danych wśród cyberprzestępców. Twoją czujność powinny wzbudzić podejrzane linki przekierowujące na stronę płatności, sugerujące o dopłatach, braku realizacji transakcji, itp. Często takie przekserowanie to próba wyłudzenia danych do logowania na stronie, która do złudzenia przypomina stronę Twojego banku.

7. PAMIĘTAJ O AKTUALIZOWANIU SYSTEMU, ORAZ OPROGRAMOWANIA NA SWOIM URZĄDZENIU

ZAWSZE pamiętaj o aktualizacji systemu i oprogramowania antywirusowego. Systemy pełne są „dziur", przez które cyberprzestępcy mogą się dostać do Twojego konta, dlatego tak ważne są uaktualnienia, które te „dziury" naprawiają. Z kolei oprogramowanie antywirusowe na wczesnym etapie pozwala wykryć złośliwe oprogramowanie i zabezpieczyć Twoje urządzenie mobilne przed atakiem cyberprzestępcy.

Literatura:

1. Anderson R., Inżynieria zabezpieczeń, Wydawnictwa Naukowo-Techniczne, Warszawa 2005
2. Cole E., Krutz R. L., Conley J., Bezpieczeństwo sieci - Biblia, Wydawnictwo HELION, Gliwice 2005
3. Gibson,W., Neuromancer. Katowice: Wydawnictwo Książnica 2009
4. Kontselidze A., Cyberterrorism – when technology became a weapon, „European Scientific Journal" 2015
5. Negroponte J. D., Palmisano S.J., Segal A., Defending an Open, Global, Secure, and Resilient Internet, Nowy Jork 2013
6. Nowakowski, Z., Szafran H., Szafran R., Bezpieczeństwo w XXI wieku. Strategie bezpieczeństwa narodowego Polski i wybranych państw. Rzeszów: Politechnika Rzeszowska 2009
7. Strebe M., Bezpieczeństwo sieci - podstawy, Wydawnictwo MIKOM, Warszawa 2005
8. Webster W., Cilluffo F., Cybercrime Cyberterrorism Cyberwarfare: Averting an Electronic Waterloo, Waszyngton 1998