Jak walczyć z informacją/dezinformacją w trudnym wojennym okresie?

Choć wojny stale toczą się w różnych zakątkach świata, to od wielu lat bezpośrednia inwazja na inne państwo nie dotyczyła Polski w tak znaczącym stopniu, jak dzieje się to obecnie. Jako naród wzorowo zdajemy egzamin z człowieczeństwa pomagając uchodźcom z Ukrainy - ale trzeba pamiętać, że wojna toczy się również w internecie.

Chcesz pomóc? Pamiętaj, aby weryfikować prawdziwość zbiórek pieniędzy

Zaczniemy od problemu, który bezpośrednio może uderzyć w Twoje finanse. Dezinformację wykorzystują cyberprzestępcy, którzy mają świadomość panujących teraz nastrojów społecznych i chęci społeczeństwa do finansowego wsparcia Ukrainy. Zakładają więc oni zbiórki pieniędzy, z których dochód rzekomo ma trafić na uchodźców. Choć na pierwszy rzut oka mogą wyglądać one prawdziwie, to służą do wyłudzania pieniędzy.

Podobnie trzeba uważać na wszelkie SMS-y, e-maile, wiadomości w social mediach czy telefony, w których dane instytucje (lub osoby podszywające się pod nie) oferują możliwość wsparcia finansowego dla Ukrainy. Przed kliknięciem w link przekierowujący do innej strony należy sprawdzić, jaki jest jej adres docelowy - jeśli tego nie zrobisz, możesz nieintencjonalnie pobrać złośliwe oprogramowanie.

Jak nie dać się oszukać, a dzięki temu realnie pomóc ofiarom wojny?

- Korzystaj tylko ze sprawdzonych źródeł i zawsze weryfikuj, jaki podmiot prowadzi akcję charytatywną.
- Nie klikaj bezmyślnie we wszystkie linki do zbiórek udostępnianych w social mediach - masowe udostępnianie bez weryfikacji to siła napędowa cyberprzestępców.
- Zawsze sprawdzaj adres URL strony, na którą zostaniesz przekierowany - szczególnie jeśli chodzi o płatność. Nie kieruj się tylko jej layoutem, ponieważ może on zostać skopiowany przez hakerów.

Codziennie spotykamy się z udostępnionymi tragicznymi obrazami z wojny - pomagajmy więc potrzebującym, ale pamiętajmy też, że to czas intensywnych działań hakerów. Niech więc emocje nie przeważają nad zdrowym rozsądkiem, jeśli chodzi o cyberbezpieczeństwo.

Weryfikuj także informacje, jeszcze zanim przekażesz je dalej

Wojna trwa także w sieci - i o ile w poprzednim przykładzie nawiązaliśmy do „zwykłych" cyberprzestępców chcących wzbogacić się na tragedii, o tyle w kwestii informacyjnej trzeba uważać na prawdopodobne akcje rosyjskich służb. Przykładem jest oczywiście sytuacja z pierwszych dni agresji na Ukrainę, gdy w Polsce viralowo rozprzestrzeniła się wiadomość o tym, że za kilka dni zabraknie paliwa na stacjach benzynowych. Informacja poszła w eter i to wystarczyło, aby ludzie masowo ruszyli do dystrybutorów.

Takie działania dezinformacyjne mają wprowadzać chaos, niepewność, nieufność oraz podziały w danym społeczeństwie. Z czasem może ich być więcej, dlatego trzeba wiedzieć, jak się przed nimi chronić.

Najważniejszą zasadą jest czerpanie informacji tylko ze sprawdzonych źródeł. Szczególnie ważne w kontekście spraw związanych z cyberbezpieczeństwem są komunikaty publikowane przez takie podmioty jak CSIRT, KNF czy CERT. Dodatkowo pamiętaj, że jeśli zauważysz podejrzaną aktywność w sieci, możesz zgłosić ją do weryfikacji poprzez formularz na stronie CERT.

Warto z pewną dozą sceptycyzmu podchodzić do wszystkich informacji, które nie są oficjalnie potwierdzone - nawet jeśli są masowo rozpowszechnione w mediach czy social mediach. Newsy nawiązujące do cyberbezpieczeństwa Polski w czasie wojny trzeba weryfikować na portalach, które od lat zajmują się tą tematyką. Są to na przykład: Zaufana Trzecia Strona, Niebezpiecznik czy Sekurak. Przy okazji chcemy polecić bezpłatne szkolenie zorganizowane przez Sekurak, które dotyczyło właśnie tematu dezinformacji i fake newsów oraz porad, jak je rozpoznawać.

Pamiętaj, że sam masz wpływ na innych!
Rozpowszechnianie fake newsów można porównać do efektu kuli śnieżnej - początkowo informacja funkcjonująca tylko w określonym miejscu w sieci/grupie może dotrzeć do miliona osób. Choć sam nie zatrzymasz machiny dezinformacji, to jednak znacząco możesz ochronić siebie, swoją rodzinę czy znajomych przed jej konsekwencjami.

Social media są potężnym narzędziem i niestety bardzo przyczyniają się do rozpowszechniania fake newsów. Pamiętaj, aby edukować osoby w Twoim otoczeniu o potencjalnych niebezpieczeństwach w sieci i sam rozsądnie korzystaj z opcji polubień czy udostępnień. Nie wzmagaj chaosu informacyjnego - nawet jeśli dany tweet czy post wydaje się być w słusznej sprawie, viralowe udostępnianie niesprawdzonych treści może zamazywać realny obraz konfliktu.

Szczególnie zwracaj uwagę na zdjęcia czy materiały wideo, które rzekomo pokazują daną sytuację. Bardzo często spotkasz się z materiałami, które pochodzą z ubiegłych lat lub zostały wykonane w zupełnie innym miejscu, ale pasują do kontekstu wojennego. W pierwszym dniu wojny bardzo popularny był film przedstawiający rosyjskie samoloty lecące bardzo nisko nad jednym z miast w Ukrainie - był to jednak film nakręcony dużo wcześniej podczas parady wojskowej. Oczywiście zwykłemu użytkownikowi bardzo trudno zweryfikować wszystkie napływające z frontu informacje i materiały, dlatego zachęcamy do wstrzemięźliwości w ich podawaniu dalej i skupieniu się na realnej pomocy uchodźcom, którzy bardzo jej potrzebują!

Chłodna głowa w internecie to podstawa - szczególnie w obecnym czasie
Całe rozważania sprowadzają się więc do konkluzji, że najważniejszy jest dystans, odsunięcie emocji na bok i racjonalna ocena sytuacji. Machina dezinformacyjna polega na „zasypaniu" użytkownika tak dużą ilością informacji, często sprzecznych, że nie jest w stanie odróżnić on w każdym przypadku prawdy od fikcji. Z tego względu należy pamiętać o dozie sceptyzymu w przyjmowaniu zarówno negatywnych, jak i pozytywnych nieoficjalnych komunikatów.

A jeśli pojawi się niepotwierdzona informacja, która będzie zachęcała do podjęcia jakiejś czynności (na przykład do wypłaty gotówki z bankomatów) - nie ulegaj presji! Edukuj także osoby w swoim otoczeniu, jak zachować się w takiej sytuacji i dlaczego to tak ważne. Kieruj się zdrowym rozsądkiem, zamiast podążać za tłumem.

Źródło: www.fingerprints.digital

***

Biuro Informacji Kredytowej oraz BIG InfoMonitor są inicjatorami Programu edukacyjnego Nowoczesne Zarządzanie Biznesem i partnerami w module „Zarządzanie ryzykiem finansowym w biznesie i życiu osobistym".

Więcej: www.nzb.pl / www.facebook.com/NowoczesneZarzadzanieBiznesem