Informacje dotyczące bezpieczeństwa cyfrowego w związku ze zbrojną agresją na Ukrainę

Szanowni Państwo, Drodzy Uczniowie!

Jesteśmy świadkami tragedii Ukrainy, Europy i całego świata.. Przemoc zbrojna Federacji Rosyjskiej przeciw Ukrainie przynosi niezmierzony ogrom cierpień i strat. Informacje o szeregu nieszczęść napływają do nas każdego dnia, a wśród nich jest wiele, które mają w nas wzbudzać lęk, szerzyć niepokój, wprowadzać oskarżenie, a także panikę. Mamy do czynienia ze zjawiskiem fałszywych informacji (fake news), przypadkami manipulacji i całkowitej dezinformacji.

Należy zaznaczyć, że zauważono istotne działanie oszukańcze w Polsce, z uwagi na rolę Polski jako kraju, do którego uciekają przed wojną mieszkańcy Ukrainy. Szerzenie nieprawdziwych informacji mają wspólny wątek – wykorzystanie obaw związanych z wojną. Naszym celem jest zadbać o bezpieczeństwo własne, ale również naszych podopiecznych.

Korzystając z różnych platform i stron internetowych jest to ważniejsze niż kiedykolwiek wcześniej, aby stosować podstawowe praktyki mające na celu zapobieganie potencjalnemu zniekształceniu informacji w przestrzeni cyfrowej!

1. Pomyśl, zanim klikniesz! Cyberprzestępcy wykorzystują ludzi szukających informacji na temat wojny. Rozpowszechniają fałszywe informacje, wiadomości, numery kont bankowych ze złośliwym oprogramowaniem, podając się za organizacje humanitarne, w celu wyłudzenia pieniędzy. Wejdź na stronę internetową organizacji, która jest zweryfikowana i prowadzi wiarygodną zbiórkę lub pomoc. Korzystaj ze sprawdzonych numerów telefonów.
2. Dezinformację charakteryzuje motywacja polityczna, która celowo wprowadza w błąd, aby szerzyć nieufność wobec działań podejmowanych przez Państwo Polskie. Szczególnie niebezpieczne jest powielanie tego typu informacji, które mogę **destabilizować kraj!**

3. Nie podawaj plotek, pogłosek i nie potęguj zamieszania. W mediach społecznościowych trzeba szczególnie uważać na udostępniane treści. Korzystaj z zaufanych źródeł i sam również bądź takim źródłem dla swoich bliskich, znajomych i społeczeństwa.
4. Sensacyjne hasła i skrajne emocje dotyczące m.in. zamknięcia sklepów, braku pieniędzy w bankach, braku paliwa na stacjach benzynowych mają przykuć uwagę. Jest to tzw. **clickbait**, którego zadaniem jest wygenerować ruch na stronie, która jest bardzo często przepełniona reklamami.
5. Przeczytaj artykuł zanim go skomentujesz. Zwróć uwagę jakim językiem napisano artykuł, lub jakie zdjęcia zamieszczono. Fotomontaż można wykonać w kilka minut. Sprawdź źródło, autora, grafikę.

Komunikując się pocztą elektroniczną, pamiętaj o bezpieczeństwie swoich danych.

1. **Uważaj na załączniki.** Nigdy nie otwieraj załączników od nieznanych nadawców. Załączniki często zawierają złośliwą treść. Jeśli znajduje się w wiadomości niespodziewany załącznik, zweryfikuj go u nadawcy przed jego otwarciem.
2. **Unikaj e-maili, które nalegają na niezwłoczne działanie.** Takie wiadomości próbują często tworzyć poczucie pilności i szybkiego działania. Ich celem jest to, aby kliknąć w link i podać natychmiast dane osobowe. Należy niezwłocznie usunąć wiadomość.
3. **Sprawdzaj adres mailowy oraz link.** Możesz sprawdzić link, najeżdżając kursorem myszy na adres URL i zobaczyć, gdzie on prowadzi. Czasami jest to oczywiste, że adres strony internetowej nie jest autentyczny. Ale pamiętaj, że oszuści potrafią stworzyć linki, które bardzo przypominają autentyczne adresy. Jeśli masz wątpliwości, nie klikaj w link.
4. **Zwracaj uwagę na pisownię i błędy gramatyczne.** Jeżeli w e-mailu znajdują się błędy w pisowni, interpunkcji lub błędy gramatyczne, prawdopodobnie otrzymałeś e-mail z potencjalnym oszustwem.
5. **Jeśli e-mail wydaje się podejrzany**, niezwłocznie usuń go lub poinformuj o tym odpowiedniego administratora strony, serwisu lub służby odpowiedzialnej za bezpieczeństwo.
6. **Bądź świadomy** obecnie krążących zagrożeń i oszustw w związku z tym kryzysem poprzez okresowe przeglądy za pomocą programów do wykrywania zagrożeń dla ogólnoświatowego bezpieczeństwa IT, które obejmuje zagrożenia dla bezpieczeństwa cyfrowego.

Chroń informacje i zasoby związane z pracą i życiem osobistym.

1. **Korzystaj z bezpiecznych połączeń Wi-Fi.** Łącz się tylko z bezpiecznymi sieciami publicznymi i prywatnymi. Nigdy nie łącz się z niezabezpieczonymi lub nieznanymi sieciami Wi-Fi.
2. **Twórz mocne hasła.** Mocne hasła nie tylko ochronią Twoje urządzenia i systemy, do których masz dostęp, gdy telefon lub laptop zostaną skradzione, ale także chronią przed hakerami. Praktyki dobrych haseł obejmują używanie długich haseł z wieloma znakami, dwuetapowe procesy uwierzytelnienia oraz unikalne hasła dla różnych systemów i loginów. Nie zapisuj haseł w komputerze!
3. **Ogranicz dostęp do urządzenia, na którym pracujesz.** Rodzina i przyjaciele nie powinni korzystać z urządzenia przeznaczonego do pracy.
4. **Chroń urządzenia mobilne i laptopy.** Kradzież jest nie tylko niedogodnością, ale również potencjalnie oznacza także utratę ważnych informacji oraz danych.
5. **Zawsze wyłączaj laptopa na noc.** Pozwoli to m.in. na regularne aktualizowanie Twojego systemu operacyjnego lub programów.
6. **Uważaj na to, co pobierasz.** Najważniejszym celem oszustów jest nakłonienie Cię do pobrania złośliwego oprogramowania lub aplikacji, które zawierają złośliwe oprogramowanie lub próbują wykraść Twoje informacje. To złośliwe oprogramowanie może być zamaskowane jako popularna aplikacja. Nie pobieraj aplikacji, które wyglądają na podejrzane lub pochodzą ze strony, której nie ufasz.

Ofiary ataków w sieci mogą doświadczyć depresji, zaburzeń lękowych i emocjonalnych. O sytuacji należy poinformować rodzinę, szkołę lub administratorów sieci. Konieczne jest podjęcie działań wychowawczych i kontakt ze specjalistami w zakresie bezpieczeństwa cyfrowego. Nie bój się prosić o pomoc!

ZESPÓŁ DS. CYBERBEZPIECZEŃSTWA SZKOŁY

Opracował: mgr inż. Paweł Sosnówka