Informacje dotyczące bezpieczeństwa IT w związku z pandemią COVID-19

Drodzy Państwo,

obecnie firmy, instytucje w tym szkoły mogą być narażone na zwiększony poziom celowych ataków cybernetycznych. Należy zaznaczyć, że zauważono istotną działalność oszukańczą na całym świecie. Wszystkie działania mają wspólny wątek – wykorzystanie obaw związanych z kryzysem zdrowotnym. Naszym celem jest zadbać o bezpieczeństwo własne, ale również naszych podopiecznych.

Prowadząc zdalne zajęcia w oparciu o różne platformy i strony internetowe jest to ważniejsze niż kiedykolwiek wcześniej, aby stosować podstawowe praktyki mające na celu zapobieganie potencjalnym atakom na zasoby danych osobowych!

1. Pomyśl, zanim klikniesz. Cyberprzestępcy wykorzystują ludzi szukających informacji na temat COVID-19. Rozpowszechniają kampanie ze złośliwym oprogramowaniem, podając się za takie organizacje jak WHO, CDC i inne uznane źródła oraz prosząc o kliknięcie w linki lub pobranie map ognisk. Powoli. Nie klikaj. Wejdź na uznaną stronę internetową, aby uzyskać dostęp do treści.

Zanim otworzysz email sprawdź, czy nie ma podejrzanych wskazówek. Zadaj sobie pytania:

Czy znam tego nadawcę?

Czy spodziewałem/am się tej wiadomości?

Czy spodziewałem/am się załącznika?

Jeśli na którekolwiek z tych pytań odpowiedź brzmi „nie”, uznaj wiadomość za podejrzaną i zachowaj ostrożność!

Po otwarciu wiadomości:

Sprawdź, czy znajdują się w niej ogólne pozdrowienia. To mało prawdopodobne, aby e-maile z phishingiem* używały Twojego imienia. Pozdrowienia typu „Szanowny Panie/Szanowna Pani” mogą wskazywać, że e-mail nie jest autentyczny.

Uważaj na załączniki. Nigdy nie otwieraj załączników od nieznanych nadawców. Załączniki często zawierają złośliwą treść. Jeśli otrzymałeś/aś niespodziewany załącznik, zweryfikuj go u nadawcy przed jego otwarciem. Jeśli otrzymałeś/aś wiadomość przez e-mail, zweryfikuj ją przez telefon.

Unikaj e-maili, które nalegają na natychmiastowe działanie. E-maile z phishingiem próbują często tworzyć poczucie pilności i szybkiego działania. Ich celem jest to, abyś kliknął/ęła w link i podał/a dane osobowe – natychmiast. Usuń wiadomość.

Uważaj na żądanie danych osobowych online. E-mail, którego tematem jest koronawirus i w którym wymaga się danych osobowych, takich jak Twój numer PESEL lub informacje dotyczące loginu, to oszustwo typu phishing. Uznane agencje rządowe nie proszą o takie informacje. Nigdy nie odpowiadaj na e-maile, podając dane osobowe czy poświadczenie logowania.

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 phisherzy potrafią stworzyć linki, które bardzo przypominają autentyczne adresy. Jeśli masz wątpliwości, nie klikaj w link.

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 phishingiem. Usuń go.

Informuj. Jeśli e-mail wydaje się podejrzany, niezwłocznie usuń go lub poinformuj o tym odpowiedniego administratora strony, serwisu lub służby odpowiedzialnej za bezpieczeństwo.

*Phishing – metoda oszustwa, w której przestępca podszywa się pod inną osobę lub instytucję w celu wyłudzenia poufnych informacji (np. danych logowania, danych karty kredytowej), zainfekowania komputera szkodliwym oprogramowaniem czy też nakłonienia ofiary do określonych działań.

2. 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 nie tylko zagrożenia związane z tą pandemią, ale także inne zagrożenia dla bezpieczeństwa cyfrowego.

3. Przestrzegaj poniższych wskazówek, jeżeli pracujesz zdalnie, aby chronić informacje i zasoby:

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.

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.

Ogranicz dostęp do urządzenia, na którym pracujesz. Rodzina i przyjaciele nie powinni korzystać z urządzenia przeznaczonego do pracy.

Chroń urządzenia mobilne i laptopy. Kradzież jest nie tylko niedogodnością, ale również potencjalnie oznacza także utratę ważnych informacji oraz danych.

Zawsze wyłączaj laptopa na noc. Pozwoli to m.in. na regularne aktualizowanie Twojego systemu operacyjnego lub programów.

Uważaj na to, co pobierasz. Najważniejszym celem cyberprzestępców jest nakłonienie Cię do pobrania złośliwego oprogramowania – programów lub aplikacji, które zawierają złośliwe oprogramowanie lub próbują wykraść Twoje informacje. To złośliwe oprogramowanie może być zamaskowane jako aplikacja: od popularnej gry do czegoś, co sprawdza prognozę pogody. Nie pobieraj aplikacji, które wyglądają na podejrzane lub pochodzą ze strony, której nie ufasz.