Aktualne ostrzeżenie dotyczące cyberbezpieczeństwa dla mieszkańców i jednostek Gminy Skrwilno

Aktualizacja: 24 lipca 2026 r.

Urząd Gminy w Skrwilnie przekazuje aktualne informacje o zagrożeniach cyberbezpieczeństwa wskazywanych przez CERT Polska, Ministerstwo Cyfryzacji oraz inne instytucje odpowiedzialne za bezpieczeństwo w sieci.

Celem komunikatu jest spokojne i praktyczne ostrzeżenie mieszkańców, pracowników Urzędu Gminy, jednostek organizacyjnych, szkół, lokalnych przedsiębiorców oraz organizacji społecznych przed najczęściej obserwowanymi metodami działania cyberprzestępców.

Najważniejsze aktualne zagrożenia

1. Fałszywe wiadomości o zwrocie podatku, nadpłacie lub przyznanym świadczeniu

Cyberprzestępcy nadal rozsyłają wiadomości podszywające się pod Krajową Administrację Skarbową i e-Urząd Skarbowy. W wiadomościach pojawia się informacja o rzekomym zwrocie podatku, nadpłacie albo konieczności odebrania pieniędzy.

Obserwowane są również podobne kampanie wykorzystujące wizerunek innych instytucji i przedsiębiorstw, np. Narodowego Funduszu Zdrowia lub dostawców energii elektrycznej.

Link umieszczony w wiadomości prowadzi do fałszywej strony, której celem jest wyłudzenie danych osobowych, danych karty płatniczej albo danych logowania.

Przed podaniem jakichkolwiek danych należy samodzielnie wejść na oficjalną stronę danej instytucji, wpisując jej adres w przeglądarce. Nie należy korzystać z linków przesłanych w niespodziewanych wiadomościach.

2. Fałszywe wiadomości o przesyłkach, opłatach drogowych i parkingowych

Aktualnie obserwowane są wiadomości podszywające się pod firmy kurierskie, operatorów parkingów oraz system e-TOLL.

Wiadomości mogą informować o:

- konieczności potwierdzenia danych przesyłki;
- niedopłacie za dostarczenie paczki;
- nieudanej próbie doręczenia;
- nieopłaconym parkingu;
- nieuregulowanej opłacie za przejazd drogą płatną.

Link prowadzi najczęściej do fałszywej strony wyłudzającej dane osobowe i dane karty płatniczej.

Status przesyłki, opłaty drogowej albo parkingowej należy sprawdzać wyłącznie w oficjalnej aplikacji lub na stronie właściwego operatora, otwartej samodzielnie przez użytkownika.

3. Fałszywe wiadomości od banków i serwisów płatniczych

Cyberprzestępcy podszywają się pod banki i operatorów płatności. Wiadomości mogą informować o rzekomej konieczności:

- potwierdzenia danych;
- aktywacji nowych zabezpieczeń;
- odblokowania konta;
- potwierdzenia nietypowej transakcji;
- pilnej weryfikacji rachunku.

Po kliknięciu w link użytkownik może trafić na stronę podobną do prawdziwego serwisu bankowości elektronicznej. Podanie loginu, hasła, kodu SMS, danych karty albo kodu BLIK może doprowadzić do utraty pieniędzy.

Do bankowości elektronicznej należy logować się wyłącznie przez oficjalną aplikację bankową albo samodzielnie wpisany adres strony banku.

Nie należy zatwierdzać w aplikacji bankowej transakcji BLIK, przelewu ani logowania, jeżeli nie zostały one samodzielnie zainicjowane. Przed zatwierdzeniem należy sprawdzić kwotę, odbiorcę i rodzaj operacji.

4. Fałszywe wiadomości o dezaktywacji poczty lub wygaśnięciu domeny

Obserwowane są kampanie phishingowe podszywające się pod dostawców poczty elektronicznej i administratorów domen internetowych.

Wiadomości mogą informować o:

- planowanym wyłączeniu skrzynki;
- konieczności uzupełnienia danych;
- przekroczeniu limitu miejsca;
- rzekomym podniesieniu poziomu bezpieczeństwa konta;
- wygaśnięciu domeny internetowej;
- konieczności pilnego przedłużenia usługi.

Celem takiego ataku jest przejęcie loginu i hasła do poczty, danych osobowych, a niekiedy również danych karty płatniczej.

Przejęta skrzynka może zostać wykorzystana do wysyłania fałszywych wiadomości do znajomych, kontrahentów, pracowników, urzędów lub firm.

W przypadku wątpliwości należy zalogować się do poczty lub panelu domeny w zwykły sposób, bez korzystania z linku zawartego w otrzymanej wiadomości.

5. Fałszywe zamówienia, faktury i dokumenty w załącznikach

Cyberprzestępcy przesyłają wiadomości wyglądające jak zwykła korespondencja biznesowa. Mogą one dotyczyć rzekomego:

- zamówienia lub zapytania ofertowego;
- potwierdzenia wpłaty;
- rozliczenia płatności;
- dokumentu do podpisu;
- dokumentu wymagającego opieczętowania;
- wezwania do zapłaty lub zaległej faktury.

Załącznik może zawierać złośliwe oprogramowanie umożliwiające kradzież danych, przejęcie komputera albo uzyskanie zdalnego dostępu do urządzenia.

Szczególną ostrożność należy zachować wobec:

- archiwów, np. plików ZIP i RAR;
- plików wykonywalnych i skryptów, np. EXE, MSI, BAT, CMD lub SCR;
- plików, których nazwa ma udawać zwykły dokument;
- dokumentów żądających włączenia makr lub dodatkowej zawartości.

Przed otwarciem nieoczekiwanego załącznika należy potwierdzić jego autentyczność, kontaktując się z nadawcą za pomocą znanego wcześniej numeru telefonu albo danych kontaktowych samodzielnie znalezionych na oficjalnej stronie firmy.

6. Przejęcia kont i podszywanie się pod inne osoby w komunikatorach

Cyberprzestępcy próbują przejmować konta w komunikatorach i mediach społecznościowych. Mogą również tworzyć fałszywe konta z imieniem, nazwiskiem oraz zdjęciem znanej osoby.

W przypadku komunikatora Signal odnotowano kampanie, w których przestępcy podszywali się pod obsługę techniczną aplikacji i informowali o rzekomej blokadzie konta. Celem było nakłonienie użytkownika do kliknięcia w złośliwy link i przejęcie kontroli nad jego komunikacją.

Po przejęciu konta oszuści mogą wysyłać do kontaktów ofiary prośby o:

- pilny przelew;
- kod BLIK;
- przekazanie danych;

- otwarcie dokumentu;
- kontakt z inną wskazaną osobą;
- wykonanie nietypowej dyspozycji służbowej lub finansowej.

Każdą nietypową prośbę od przełożonego, dyrektora, pracownika urzędu, osoby publicznej, znajomego lub kontrahenta należy potwierdzić innym kanałem, najlepiej telefonicznie pod znanym wcześniej numerem.

Zalecenia dla mieszkańców

- Nie klikaj w linki zawarte w podejrzanych lub niespodziewanych wiadomościach SMS, e-mailach i komunikatorach.
- Nie podawaj loginu, hasła, kodu SMS, kodu BLIK ani danych karty na stronie otwartej z linku przesłanego w wiadomości.
- Loguj się do banku, poczty, e-Urzędu Skarbowego, Profilu Zaufanego, ePUAP, e-Doręczeń i pozostałych usług publicznych wyłącznie przez oficjalne strony lub aplikacje.
- Sprawdzaj dokładnie adres strony internetowej, szczególnie jej nazwę domenową.
- Nie działaj pod presją czasu. Oszuści często używają określeń takich jak: „pilne", „ostatni termin", „blokada konta", „zwrot pieniędzy" lub „natychmiastowa weryfikacja".
- Nie zatwierdzaj w aplikacji bankowej operacji, której samodzielnie nie rozpocząłeś.
- Stosuj różne hasła do różnych usług i włącz uwierzytelnianie wieloskładnikowe wszędzie tam, gdzie jest dostępne.
- Podejrzany SMS można przekazać do CERT Polska na bezpłatny numer **8080**, korzystając z funkcji „Przekaż" lub „Udostępnij".
- Podejrzane strony, wiadomości e-mail i oszustwa można zgłaszać przez formularz zgłoszeniowy CERT Polska albo przez usługę „Bezpiecznie w sieci" w aplikacji mObywatel.
- W przypadku podejrzenia utraty pieniędzy należy niezwłocznie skontaktować się z bankiem i zawiadomić Policję.

Zalecenia dla pracowników Urzędu Gminy i jednostek organizacyjnych

- Nie otwieraj nieoczekiwanych załączników dotyczących faktur, płatności, przelewów, zamówień lub dokumentów do podpisu bez potwierdzenia nadawcy.
- Każdą nietypową dyspozycję płatniczą, zmianę numeru rachunku bankowego albo pilną prośbę o przekazanie danych potwierdzaj innym kanałem.

- Nie przekazuj informacji służbowych, danych osobowych ani dyspozycji finansowych przez prywatne lub niezatwierdzone przez urząd komunikatory.
- Korzystaj wyłącznie z narzędzi i kanałów komunikacji dopuszczonych przez urząd lub jednostkę.
- Nie udostępniaj innym osobom kodów uwierzytelniających ani powiadomień służących do zatwierdzania logowania.
- Stosuj silne, unikalne hasła i uwierzytelnianie wieloskładnikowe.
- Każdy podejrzany e-mail, telefon, komunikat lub nietypowe zachowanie komputera niezwłocznie zgłaszaj przełożonemu albo osobie odpowiedzialnej za obsługę informatyczną.
- Nie usuwaj samodzielnie podejrzanych plików, wiadomości ani śladów zdarzenia, jeżeli mogą być potrzebne do analizy incydentu.
- Zgłoszenie wiadomości do CERT Polska nie zastępuje wewnętrznego zgłoszenia incydentu zgodnie z procedurami obowiązującymi w Urzędzie Gminy lub jednostce organizacyjnej.

Zalecenia dla administratorów systemów

Administratorzy powinni w szczególności:

- prowadzić aktualną inwentaryzację urządzeń, systemów, domen, kont i usług dostępnych z Internetu;
- regularnie aktualizować systemy operacyjne, urządzenia sieciowe, zapory, systemy VPN, serwery pocztowe, systemy CMS, panele administracyjne oraz oprogramowanie do kopii zapasowych;
- wyłączyć dostęp do paneli administracyjnych bezpośrednio z Internetu, jeżeli nie jest on niezbędny;
- zabezpieczyć dostęp zdalny za pomocą VPN i uwierzytelniania wieloskładnikowego;
- ograniczyć możliwość zarządzania urządzeniami do zaufanych adresów IP;
- regularnie przeglądać konta uprzywilejowane, logi systemowe, zdarzenia bezpieczeństwa i historię zmian konfiguracji;
- stosować segmentację sieci;
- wycofywać lub wymieniać urządzenia i oprogramowanie, dla których producent zakończył wsparcie;
- regularnie wykonywać kopie zapasowe oraz testować możliwość rzeczywistego odtworzenia danych;
- chronić przynajmniej jedną kopię zapasową przed zmianą lub usunięciem z poziomu podstawowej sieci organizacji;

- monitorować komunikaty producentów, CERT Polska, CSIRT NASK i Ministerstwa Cyfryzacji dotyczące nowych podatności.

Co zrobić w przypadku podejrzenia incydentu

W przypadku kliknięcia w podejrzany link, podania danych logowania, uruchomienia podejrzanego załącznika, przejęcia konta albo utraty pieniędzy należy:

1. Przerwać dalsze działania na podejrzanej stronie.
2. Nie podawać kolejnych danych ani kodów autoryzacyjnych.
3. Nie zatwierdzać kolejnych operacji w aplikacji bankowej.
4. W przypadku podania danych bankowych lub karty natychmiast skontaktować się z bankiem.
5. Z bezpiecznego urządzenia zmienić przejęte hasło oraz hasła do innych usług, w których użyto tego samego hasła.
6. Wylogować aktywne sesje na przejętym koncie i włączyć uwierzytelnianie wieloskładnikowe.
7. Zgłosić podejrzaną wiadomość, stronę lub zdarzenie do CERT Polska.
8. W przypadku straty finansowej albo podejrzenia przestępstwa zawiadomić Policję.
9. W przypadku urządzenia służbowego natychmiast powiadomić przełożonego i osobę odpowiedzialną za obsługę informatyczną.
10. Nie resetować, nie formatować ani nie czyścić samodzielnie służbowego urządzenia, chyba że takie polecenie wyda osoba odpowiedzialna za obsługę incydentu.

Źródła:

Komunikat przygotowano na podstawie bieżących ostrzeżeń CERT Polska i CSIRT NASK, informacji Ministerstwa Cyfryzacji, komunikatów publikowanych w serwisie moje.cert.pl oraz aktualnych zaleceń dotyczących zabezpieczenia urządzeń brzegowych i systemów dostępnych z Internetu.