

Transkrypcja lekcji: Trzy oszustwa, które trafiają do placówek

Dla dyrektorów, opiekunek i wszystkich osób, które w placówce odbierają telefony, faktury i wiadomości od rodziców.

Cyfrowy żłobek, moduł 2, lekcja 2.2 · nagranie 11 minut · znaczniki czasu są przybliżone i odnoszą się do początku każdej części nagrania

0:00 1. Tytuł lekcji

Dzień dobry Państwu. Nazywam się Tomasz Stelmach. Zapraszam na drugą lekcję modułu o cyberhigienie w placówce. Temat brzmi: trzy oszustwa, które trafiają do placówek. Najbliższe kilkanaście minut poświęcimy na to, żeby rozpoznawali je Państwo już po pierwszym zdaniu wiadomości.

0:18 2. Skala zjawiska

Zacznę od tego, kim jestem, bo to tłumaczy, skąd biorę przykłady. Pracuję z jakością i bezpieczeństwem oprogramowania od ponad piętnastu lat. Kieruję firmą Quality Island. Mój zespół ogląda systemy od środka i szuka w nich słabych miejsc, zanim znajdzie je ktoś inny.

Teraz jedna liczba. CERT Polska, czyli zespół reagowania na incydenty działający w NASK, przyjął w dwa tysiące dwudziestym piątym roku sześćset pięćdziesiąt osiem tysięcy trzysta dwadzieścia zgłoszeń. To dane z raportu rocznego opublikowanego w kwietniu tego roku.

I druga liczba z tego samego raportu. Dziewięćdziesiąt siedem procent zarejestrowanych incydentów to były oszustwa komputerowe. Nie awarie, nie włamania do serwerowni. Oszustwa na człowieka.

1:06 3. Dlaczego placówka

Dlaczego mówię o tym akurat Państwu.

W komputerze i w telefonie placówki są dane dzieci i rodziców. Imiona, adresy, numery telefonów, czasem informacje o zdrowiu i o alergiach.

Są tam pieniądze. Faktury za posiłki, opłaty od rodziców, przelewy.

I jest zaufanie. Rodzic wierzy, że wiadomość z placówki jest prawdziwa, a Państwo wierzą, że wiadomość od rodzica jest prawdziwa.

Stąd najważniejsze zdanie tej lekcji. Oszust nie atakuje żłobka. Oszust atakuje człowieka w pośpiechu. Dlatego uderza o piętnastej czterdzieści, kiedy trwa odbiór dzieci i dzwoni telefon.

1:47 4. Plan lekcji

Pokażę Państwu trzy schematy. Zawsze te same trzy trafiają do placówek.

Pierwszy: podmiana numeru rachunku. Wiadomość od dostawcy, że zmienił konto.

Drugi: SMS o dopłacie do przesyłki albo o zaległej opłacie, z linkiem do fałszywej płatności.

Trzeci: to mój nowy numer. Ktoś podszywa się pod rodzica albo pod dyrektora w komunikatorze.

Każdy rozłożył tak samo: jak wygląda, po czym go poznać, co zrobić w sześćdziesiąt sekund i jak ustawić procedurę, żeby to się nie powtórzyło.

2:25 5. Oszustwo pierwsze, tak to wygląda

Oszustwo pierwsze. Tak to zwykle wygląda.

Do placówki przychodzi mail od dostawcy posiłków. Nadawca się zgadza, nazwa firmy się zgadza, stopka się zgadza.

Treść jest spokojna i uprzejma. Zmieniliśmy bank, prosimy o opłacenie faktury na nowy rachunek, przepraszamy za zamieszanie.

W załączniku jest faktura. Ten sam układ, ten sam znak firmowy, ta sama kwota co zawsze. Zmieniony jest jeden wiersz: numer konta. Policja opisuje ten schemat od lat i mówi wprost, że wiadomość potrafi przyjść z przejętej skrzynki prawdziwego kontrahenta. Wtedy adres nadawcy naprawdę jest prawdziwy.

3:06 6. Oszustwo pierwsze, trzy sygnały

Po czym to poznać. Trzy sygnały.

Pierwszy: zmiana numeru rachunku ogłoszona mailem. Prawdziwy dostawca też czasem zmienia bank, ale to jest dokładnie ten moment, w którym podnosimy słuchawkę.

Drugi: pośpiech i termin. Prosimy o pilne opłacenie, płatność jest po terminie, dziś ostatni dzień. Pośpiech to narzędzie pracy oszusta.

Trzeci: drobna różnica w adresie nadawcy. Jedna litera, inna końcówka, mail wyrwany z dotychczasowej rozmowy. Tylko proszę pamiętać, że Policja pisze wprost: sprawdzenie samego adresu nadawcy nie wystarczy.

3:43 7. Oszustwo pierwsze, sześćdziesiąt sekund

Co zrobić w sześćdziesiąt sekund.

Przez pierwsze dwadzieścia sekund nie płacimy. Odkładamy fakturę na bok. Żadna faktura nie jest tak pilna, jak twierdzi mail.

Przez kolejne trzydzieści sekund dzwoniemy do dostawcy. Nie pod numer z tego maila i nie pod numer z tej faktury. Pod numer z umowy albo ze starej kartoteki.

Ostatnie dziesięć sekund to jedno pytanie: czy zmienili Państwo numer konta. Jeśli usłyszymy, że nie, przekreślamy nowy numer, płacimy na stary i mówimy o tym dyrektorowi.

4:20 8. Oszustwo pierwsze, procedura

Jak ustawić to na stałe, żeby nie zależeć od czyjejś czujności w piątek po południu.

Zasada pierwsza: zmiana numeru rachunku wyłącznie po telefonie na znany numer. Znany, czyli zapisany w umowie albo w kartotece, nie ten z wiadomości.

Zasada druga: zasada dwóch osób. Przelew powyżej kwoty, którą Państwo ustalą, zatwierdzają dwie osoby. Dwie osoby rzadko śpieszą się w tym samym momencie.

Zasada trzecia: numery kont dostawców trzymamy w jednym miejscu w placówce i to miejsce jest źródłem prawdy. Nie skrzynka mailowa.

4:59 9. Oszustwo drugie, tak to wygląda

Oszustwo drugie. Telefon służbowy, godzina piętnasta czterdzieści.

Przychodzi SMS. Paczka czeka w magazynie, brakuje dopłaty jeden złoty dziewięćdziesiąt dziewięć, prosimy kliknąć, żeby dokończyć.

Albo wersja druga: zaległa opłata, konto zostanie zablokowane, prosimy o uregulowanie.

Pod linkiem jest strona, która wygląda jak bramka płatności. CERT Polska opisuje to tak: strona jest prawie identyczna z prawdziwą, a jedyna różnica to adres domenowy. I dodaje rzecz najważniejszą. Te kilka złotych to tylko pretekst. Naprawdę chodzi o dane karty i dane logowania.

5:37 10. Oszustwo drugie, trzy sygnały

Trzy sygnały.

Pierwszy: drobna kwota. Złotówka, dwa złote, pięć złotych. Przy takiej kwocie nikt nie dzwoni i nikt nie sprawdza, a dokładnie o to chodzi.

Drugi: link w SMS. Prawdziwy przewoźnik nie potrzebuje, żeby klikali Państwo w link i wpisywali dane karty. Stan przesyłki sprawdza się w aplikacji albo na stronie, którą wpisujemy sami.

Trzeci: groźba. Przesyłka wróci do nadawcy, konto zostanie zablokowane, sprawa trafi do windykacji. CERT Polska wymienia presję czasu jako pierwszy sygnał phishingu.

6:14 11. Oszustwo drugie, sześćdziesiąt sekund i procedura

Sześćdziesiąt sekund.

Nie klikamy. To całe pierwsze dziesięć sekund i najtrudniejsza część.

Przekazujemy SMS na numer osiem zero osiem zero. To bezpłatny numer CERT Polska. W telefonie wybieramy polecenie przekaż albo prześlij dalej i wysyłamy na osiem zero osiem zero. Jeśli telefon tego nie ma, kopiujemy treść i wysyłamy tak samo.

Sprawdzamy przesyłkę tam, gdzie zawsze. W aplikacji przewoźnika albo na stronie, którą wpisujemy z pamięci.

A procedura w placówce mieści się w jednym zdaniu. W placówce nie klikamy w linki płatnicze z SMS. Jeśli coś naprawdę wymaga zapłaty, robimy to z komputera, na stronie wpisanej ręcznie.

7:01 12. Oszustwo trzecie, tak to wygląda

Oszustwo trzecie i moim zdaniem najtrudniejsze, bo gra na odruchu pomagania.

W komunikatorze pojawia się wiadomość z nieznanego numeru. Dzień dobry, tu mama Zosi, zmieniłam numer, stary telefon się zepsuł.

Potem przychodzi prośba. Raz jest to pilny przelew albo kod BLIK, raz zdjęcie dokumentu, a w wersji placówkowej najczęściej: proszę dopisać ciocię do osób upoważnionych, odbierze dziś po południu.

Ta ostatnia prośba jest groźniejsza niż przelew. Przy przelewie tracimy pieniądze. Tutaj może chodzić o dziecko.

7:37 13. Oszustwo trzecie, trzy sygnały

Trzy sygnały.

Pierwszy: nowy numer i pilna prośba w jednej wiadomości. Sama zmiana numeru to normalna rzecz. Zmiana numeru razem z prośbą to już schemat.

Drugi: przenoszenie rozmowy. Z SMS na komunikator, z komunikatora na inny komunikator. Oszust ucieka z kanału, w którym można go sprawdzić.

Trzeci: presja emocjonalna zamiast argumentu. Proszę szybko, bardzo proszę, nie mam czasu tłumaczyć. Dodam jedną rzecz techniczną. Numer, który wyświetla się na ekranie, da się podrobić. Policja nazywa to spoofingiem. Sam numer nie jest dowodem tożsamości.

8:17 14. Oszustwo trzecie, sześćdziesiąt sekund i procedura

Sześćdziesiąt sekund.

Nie odpisujemy w tym samym oknie. Żadnych danych, żadnych list, żadnych kodów.

Dzwonimy pod numer z dokumentacji placówki. Nie pod ten nowy. Policja powtarza to w każdym komunikacie: jeden krótki telefon wystarczy.

Informujemy dyrektora, nawet jeśli nic się nie wydarzyło. Wiadomość, która przyszła do jednej osoby, zwykle przyszła też do kilku innych.

A procedura stoi na dwóch filarach. Pierwszy: lista osób upoważnionych do odbioru zmienia się wyłącznie na piśmie w placówce, nigdy przez wiadomość. Drugi: hasło przy odbiorze dziecka, ustalone z rodzicem i zapisane w dokumentacji. Osoba bez hasła nie odbiera dziecka. Rozwiązanie z ubiegłego wieku, a działa lepiej niż niejedna aplikacja.

9:07 15. Jedna zasada na ścianę

Teraz obiecana jedna zasada. Taka, którą warto wydrukować i powiesić w pokoju opiekunek.

Brzmi tak. Prośbę o pieniądze, o dane albo o dziecko potwierdzamy innym kanałem niż ten, którym przyszła.

I to wszystko. Przyszło mailem, dzwonimy. Przyszło SMS-em, dzwonimy. Przyszło w komunikatorze, dzwonimy. Ta jedna zasada rozbraja wszystkie trzy schematy, które dziś Państwu pokazałem, i większość tych, których jeszcze nie znamy.

9:36 16. Kogo powiadomić

Jeśli jednak ktoś kliknął, a to zdarza się w każdej organizacji, liczy się czas, nie szukanie winnego.

Bank, natychmiast. Jeśli w grę wchodzi karta albo przelew, blokujemy kartę i dzwonimy na infolinię banku.

CERT Polska. Podejrzany SMS przekazujemy na osiem zero osiem zero, a incydent zgłaszamy przez formularz na stronie incydent kropka cert kropka pe el.

Policja, jeśli doszło do oszustwa i do straty pieniędzy.

I ochrona danych. Jeśli wyciekły dane dzieci albo rodziców, ocenę robi administrator, czyli placówka, a nie pojedyncza opiekunka. Administrator zgłasza naruszenie Prezesowi Urzędu Ochrony Danych Osobowych bez zbędnej zwłoki, w miarę możliwości w ciągu siedemdziesięciu dwóch godzin od stwierdzenia, elektronicznie, przez usługę na biznes kropka gov kropka pe el. Przy wysokim ryzyku zawiadamiamy też rodziców. I rzecz, o której najczęściej się zapomina: nie kasujemy tej wiadomości przed zgłoszeniem.

10:39 17. Zakończenie

To tyle na dziś. Trzy schematy, trzy razy po sześćdziesiąt sekund i jedna zasada na ścianę. Jeśli po tej lekcji zrobią Państwo tylko jedną rzecz, niech to będzie telefon na znany numer przy następnej prośbie o pieniądze albo o dane. Dziękuję Państwu za uwagę.

Materiał wyjaśnia przepisy i dobre praktyki. Nie jest poradą prawną i nie zastępuje inspektora ochrony danych ani prawnika placówki. Stan prawny na 20.09.2026. Quality Island Sp. z o.o., ul. Grzybowska 87, 00-844 Warszawa, KRS 0000972652, NIP 5273002880. Pełna lekcja i pozostałe materiały: <https://cyfrowyzlobek.pl/lekcje-otwarte>