Informacja prasowa, 6.02.2024 r.

Dzień Bezpiecznego Internetu - jak naprawdę działają cyberprzestępcy?

**W obliczu faktu, że ponad 5 miliardów ludzi jest obecnie podłączonych do internetu, a prognozy na 2030 rok mówią o 7,5 miliardach użytkowników sieci, temat bezpieczeństwa jest aktualnie kluczowy. Metody cyberprzestępców ciągle ewoluują i dostosowują się do otaczającej nas rzeczywistości oraz bieżących wydarzeń. Całe szczęście świadomość zagrożeń zwiększa się, m.in. przez takie akcje jak Dzień Bezpiecznego Internetu, który obchodzimy dzisiaj.**

## **Jak wygląda świadomość Polaków pod względem cyberzagrożeń?**

Jednym z kluczowych aspektów, jest poziom świadomości Polaków w kontekście cyberzagrożeń. Pomimo postępu technologicznego, który umożliwia łatwiejszy dostęp do informacji oraz nagłaśnianie tematu przez media, ciągle istnieją wyzwania  związane z brakiem świadomości dotyczącej różnorodnych metod wykorzystywanych przez cyberprzestępców. Od ekspertów pytanych o ocenę tej świadomości można usłyszeć, że w pewnych kręgach jest ona zatrważająco niska.

*- Aktualnie mamy inflację różnego rodzaju systemów aplikacji i wydaje mi się, że pewna grupa społeczna nie do końca może nadążać za tym wszystkim, co się dzieje. Myślę, że łatwo się odwołać do przykładu rodziców i to wydaje mi się, że stanowi duży problem* - mówi Błażej Dusik, Starszy inżynier ds. cyberbezpieczeństwa w InternetowyKantor.pl.

-*Z kolei wykluczenie cyfrowe, przekłada się też na to, że oszustom łatwiej jest takimi osobami manipulować, bo kiedy nie znają środowiska, w którym się poruszają, kiedy nie do końca wiedzą, co jest godne zaufania, a co nie, zdecydowanie łatwiej jest je podejść i w jakiś sposób oszukać* - dodaje Kajetan Żukowski, Starszy specjalista ds. bezpieczeństwa w InternetowyKantor.pl.

## **Oszustwa a cyberataki**

Warto zwrócić uwagę na różnicę między dwoma pojęciami, czyli oszustwami skierowanymi do zwykłych obywateli a atakami cyberprzestępców wymierzanymi w firmy. Eksperci uważają, że istnieje dwufazowy model, gdzie ataki skoncentrowane na tzw. „VIP-ach” różnią się od szeroko skierowanych oszustw, które mają na celu wyłapanie jak największej ilości potencjalnych ofiar. Przykłady inwestycji w lokalne przedsięwzięcia czy kampanie podszywania się pod instytucje państwowe stanowią elementy tego złożonego krajobrazu.

*- Największym problemem jest grube sito, które wyłapuje tę masę, która jest podatna. Na przykład technologia oszustwa na deep fake, która pomimo technicznie dobrego wykonania, dla bardziej obytego użytkownika internetu jest podejrzana. Jednak w tę pułapkę mogą wpaść osoby, które nie są w stanie odróżnić tego, co ma szansę faktycznie w rzeczywistości występować od tego typu treści, które są spreparowane* - komentuje Błażej Dusik.

## **Ile warty jest biznes cyberprzestępców?**

Biznes cyberprzestępców jest dziedziną o rosnącej wartości, zyskującą na profesjonalizacji i rozbudowie struktur. Szacuje się, że w 2024 roku cyberprzestępczość będzie kosztować świat 1 miliard dolarów na godzinę. Oszuści operują w zaawansowany sposób, wykorzystując różnorodne strategie, aby osiągnąć swoje cele. Jednym z aspektów, który przyczynia się do sukcesu tego biznesu, jest skomplikowany łańcuch działań. Współczesne cyberprzestępcze działania często zaczynają się od stworzenia kampanii, która jest ukierunkowana na określoną grupę osób. To strategiczne podejście ma na celu zwiększenie skuteczności oszustwa. Zespół przygotowuje treści dostosowane do określonych kryteriów, takich jak wiek, potrzeby czy preferencje.

*- Można to trochę porównać do prężnie działającego przedsiębiorstwa - przywołując stawki, które można znaleźć niekoniecznie w tym internecie, z którego korzystamy na co dzień, ale w tych wersjach powiedzmy głębszych, to ceny za głowę, że tak nieładnie to określę, ale powiedzmy, że jesteśmy na poziomie około 800 dolarów. A to dopiero jest cena za zdobycie ofiary. Nie mówimy o tym, ile od tej ofiary się da jeszcze pozyskać* - dodaje Kajetan Żukowski.

## **Jak działają cyberprzestępcy?**

Cyberprzestępcy stosują różnorodne metody manipulacji psychologicznej, aby osiągnąć swoje cele. Najczęściej celem jest zdobycie zaufania potencjalnej ofiary. Kluczowym elementem sukcesu cyberprzestępców jest także wykorzystywanie psychologii. Przestępcy często bazują na ludzkich odruchach, takich jak chęć pomocy, unikanie problemów, czy też ciekawość co do dalszego rozwoju sytuacji. Widać to np. w przypadku fałszywych wiadomości SMS na temat dopłaty do paczki, czy od operatora energetycznego. Ponadto, elementy takie jak autorytet, zasada wzajemności czy sympatii są wykorzystywane do budowania zaufania i wprowadzania ofiar w błąd.

Cyberprzestępcy nieustannie dostosowują swoje metody do charakterystyki potencjalnych ofiar, wybierając konkretne grupy społeczne i dopasowując treści do ich potrzeb. Ostatecznym celem jest zdobycie środków finansowych, a skomplikowana struktura biznesowa cyberprzestępców sprawia, że są w stanie operować na szeroką skalę, czerpiąc zyski z różnych form oszustw.

## **Jak być bezpiecznym w sieci?**

Warto znać kilka kluczowych zasad, które warto stosować w celu zwiększenia bezpieczeństwa w cyberprzestrzeni. Jedną z nich jest koncentracja, skupienie się na danej czynności, unikanie wykonywania zadań „z doskoku”, brak pośpiechu jeżeli coś wzbudzi nasze podejrzenia i zachowanie spokoju. Ponadto, podobnie jak na drodze, w internecie warto się kierować zasadą ograniczonego zaufania. Konieczne jest również dbanie o odpowiednie hasła, aby spełniały określone warunki, jak długość, poziom skomplikowania oraz niepowtarzalność w różnych serwisach.

## **Podsumowanie**

Dzień Bezpiecznego Internetu to doskonała okazja do podniesienia świadomości na temat cyberzagrożeń. Warto pamiętać, że zagrożenia te są rzeczywiste, ewoluują i aby skutecznie się przed nimi bronić, konieczne jest ciągłe podnoszenie poziomu wiedzy społeczeństwa. Inicjatywy edukacyjne, takie jak rozmowy ekspertów czy obchody Dnia Bezpiecznego Internetu, odgrywają kluczową rolę w tym procesie, pomagając ludziom lepiej zrozumieć ryzyka związane z korzystaniem z sieci oraz umożliwiając im skuteczną ochronę swoich danych online. Powyższy artykuł jest fragmentem rozmowy, która jest w całości dostępna w podcaście serwisu InternetowyKantor.pl: Dealerzy Po Godzinach pod tytułem „Jak cyberprzestępcy wyłudzają Twoje dane i pieniądze?”, dostępnym m.in. na YouTube i Spotify.