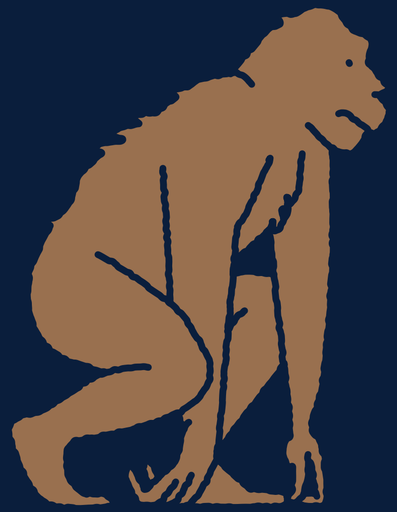
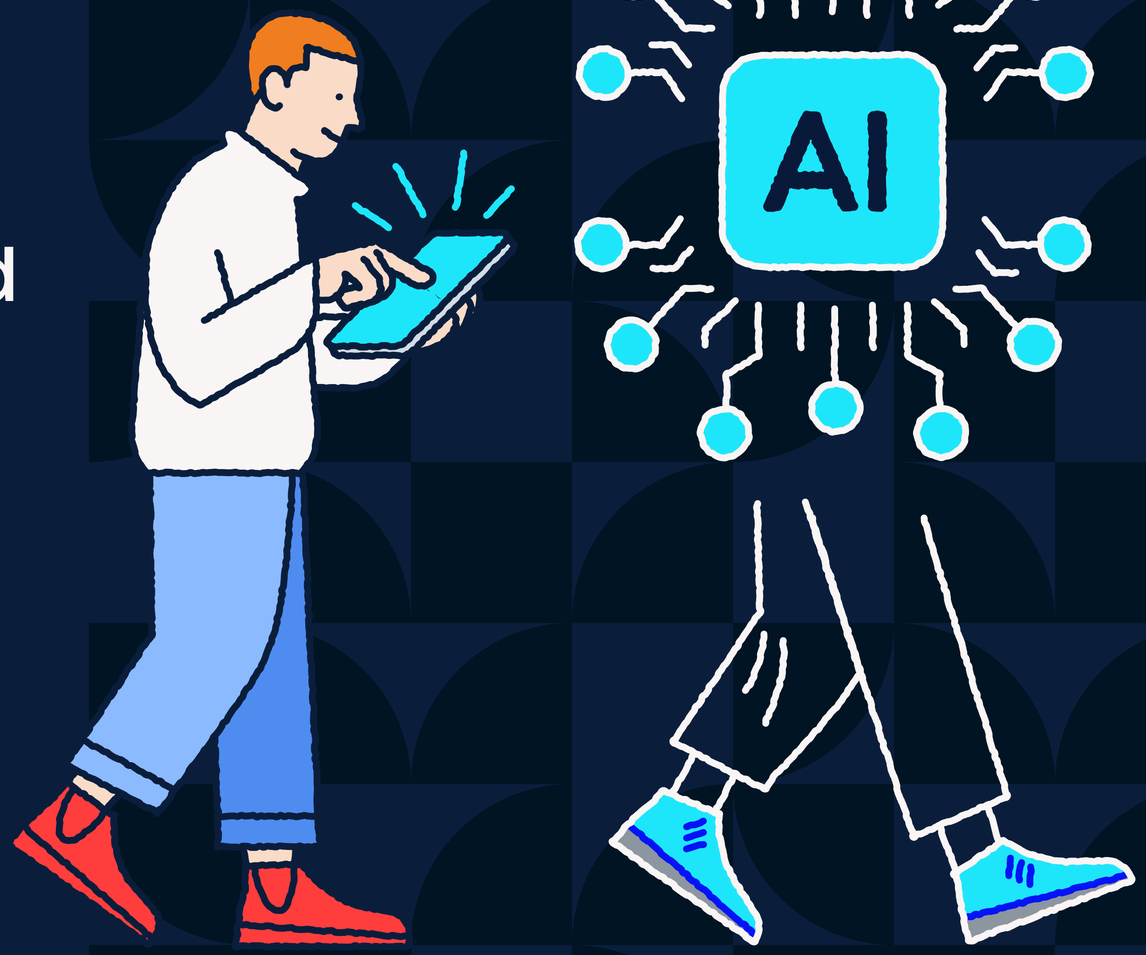
# F-Alert

Miesięczny raport o zagrożeniach od

# F-Secure

Listopad - Grudzień 2023 r.






F-Secure

# Odkryj najnowsze informacje dotyczące zagrożeń. Raport zawiera szczegółowe analizy od ekspertów z firmy F-Secure. Dostarczane co miesiąc.

Zobacz, jak oszustwa stały się najpopularniejszą formą cyberprzestępczości. Dowiedz się, w jaki sposób konsumenci są atakowani przez małe firmy. I odkryj, jak sztuczna inteligencja już teraz wywołuje kryzys wśród młodych dziewcząt.
W tym wydaniu F-Alertu na koniec roku spoglądamy wstecz na największe kryzysy związane z cyberbezpieczeństwem do tej i wybiegamy w przyszłość, aby zobaczyć, jak Nowy Rok może zmienić zarówno internet, jak i samą rzeczywistość.

PROGNOZA

# Kryzys Deepfake już nadszedł

Dziewczynki już mają do czynienia z niebezpieczeństwem fałszywych aktów AI, a dorośli muszą nadrobić zaległości.

**Dr Karolina Małagocka**
Senior Partner
Success Manager
**Warszawa, Polska**

## porada experta

Ofiary mogą spróbować skontaktować się z lokalnymi organami ścigania. W niektórych krajach, rozpowszechnianie deepfake'ów jest przestępstwem. W Polsce za rozpowszechnianie osoba posługująca się techniką deepfake'u powinna liczyć się z odpowiedzialnością za naruszenie dóbr osobistych mimowolnego „bohatera" i dotyczy to zarówno przekazów o treści erotycznej, jak i innych przeróbek jeżeli stawiają daną osobę w niekorzystynym świetle .

**"Deepfakes to technologia przeznaczona do niewłaściwego wykorzystania."**

Być może nie słyszałeś o aplikacjach, które mogą umieścić czyjąś twarz na ciele aktora w filmie pornograficznym lub "rozebrać" kogoś za pomocą sztucznej inteligencji. Ale twoje dzieci prawdopodobnie tak.

Deepfakes - obrazy lub filmy, w których jedna twarz jest zastępowana inną - istnieją od lat. Ale w ramach rewolucji generatywnej sztucznej inteligencji stają się one coraz bardziej realistyczne. A społeczeństwo nie jest przygotowane na konsekwencje.

## Koszty życia online

Deepfakes to technologia przeznaczona do niewłaściwego wykorzystania. Mogą być wykorzystywane do ataków politycznych, jako część oszustw, i do oczerniania reputacji liderów biznesu — lub prawie każdego.

Jednak najlepszym przykładem tego, jak będzie wyglądać najgorsza wersja przyszłości, jest sposób, w jaki fałszerstwa te są obecnie wykorzystywane przeciwko dziewczętom. Nowy rok szkolny przyniósł wiele przypadków rozpowszechniania fałszywych nagich zdjęć uczniów, często pozostawiając dorosłych niepewnych, jak powinni zareagować.

Wydaje się, że rozwój sztucznej inteligencji uświadomił społeczeństwu, jak łatwa w użyciu jest ta technologia. Ale sprawcy wykorzystują również to, jak wiele naszego życia jest online. Prawdopodobnie istnieje mnóstwo zdjęć, filmów i nagrań dźwiękowych, rozsianych po wielu sieciach społecznościowych, zwłaszcza jeśli dorastałeś w erze po Facebooku. Wszystko to może zostać przeniesione do innych mediów.

## Poważne traktowanie nadużyć cyfrowych

Sama sztuczna inteligencja wyłapie przynajmniej część sfałszowanych materiałów seksualnych. Narzędzia te są jednak pomocne tylko wtedy, gdy platformy internetowe biorą odpowiedzialność za materiały przesyłane przez ich użytkowników.

Platforma jest miejscem, od którego powinieneś zacząć, jeśli jesteś przedstawiony w deepfake'u rozpowszechnianym online. Niektórzy z największych dostawców usług online są również częścią inicjatywy Stop Non-Consensual Intimate Image Abuse, dzięki której możesz spróbować usunąć treści.

Ale usunięcie nie wystarczy. Otwartość na temat traumy potencjalnie spowodowanej cyfrowym wykorzystywaniem jest kluczowa. Rozmowa z kimś, komu można zaufać - niezależnie od tego, czy jest to grupa wsparcia dla ofiar wykorzystywania seksualnego, czy ukochana osoba - jest kluczem do poważnego potraktowania prawdziwego cierpienia spowodowanego przez te fałszywe filmy .

# Regulacje mogą zmienić internet

UE rozpocznie egzekwowanie ustawy o rynkach cyfrowych w celu zapewnienia uczciwej konkurencji w marcu przyszłego roku.

Ustawa o rynkach cyfrowych (DMA) może być jednym z najbardziej transformacyjnych przepisów, jakie kiedykolwiek zmieniły nasze cyfrowe życie. Dlatego poprosiliśmy Miinę Hiilloskivi-Knox, radcę prawnego w F-Secure, o przedstawienie nam przeglądu tego "centralnego elementu" przepisów, które składają się na strategię UE w zakresie danych i mającą na celu stworzenie "sprawiedliwego i otwartego" Internetu.

## Poznaj strażników bramek

Kluczowym krokiem od momentu wejścia w życie ustawy w maju 2023 r. było zidentyfikowanie tzw. strażników dostępu (ang: gatekeepers), którzy świadczą "podstawowe usługi platformowe", takie jak wyszukiwarki, systemy operacyjne i systemy reklamowe online.

"Komisja Europejska wyznaczyła Alphabet, Meta, Apple, Amazon, ByteDance i Microsoft jako gatekeeperów we wrześniu 2023 r." - powiedział Miina.

Firmy te mają czas do marca 2024 r., aby upewnić się, że ich produkty - w tym Google Maps, YouTube, Instagram, Apple AppStore, TikTok i Windows PC - są zgodne z 22 nowymi obowiązkami określonymi w rozporządzeniu.

"Ponieważ ci strażnicy działają globalnie, najprawdopodobniej zobaczymy zmiany w sposobach działania tych firm na całym świecie".

## Regulacja mocy rzeczywistej

Miina zauważył, że DMA jest znaczące, ponieważ jest to pierwsze rozporządzenie UE, które koncentruje się na regulowaniu siły największych platform cyfrowych.

"Strażnicy dostępu nie mogą preferencyjnie traktować swoich własnych ofert" - powiedziała. "DMA zabrania również śledzenia użytkowników poza podstawową platformą lub usługą oferowaną przez daną firmę, szczególnie w celach marketingowych, chyba że użytkownik wyraził na to wyraźną zgodę".

DMA zapewnia również, że użytkownicy mogą składać skargi dotyczące niezgodności z przepisami do organów publicznych.

"Jeśli wystarczająca liczba użytkowników skorzysta z tych praw, prawdopodobnie zobaczymy zmiany w sektorze rynków cyfrowych" - podsumowała.

**Miina Hiilloskivi-Knox**
Radca prawny
**Helsinki, Finlandia**

**porada experta**

Ustawa o rynkach cyfrowych nie nakłada nowych obowiązków w zakresie bezpieczeństwa na strażników dostępu, więc użytkownicy platform powinni zachować czujność online.

**"Najprawdopodobniej zobaczymy zmiany w sposobie działania tych firm na całym świecie".**

# Popularne Oszustwa

## Oszustwo związane z nieudaną dostawą

**CO:**
Oszustwa związane z nieudaną dostawą, które wykorzystują oczekiwania na niespodziewane prezenty w okresie świątecznym, istnieją od lat. Nowością jest to, że oszustwa te są coraz bardziej prawdopodobne za pośrednictwem wiadomości SMS, a nie e-mail. A teraz często zawierają one zwrot, że kierowca dostawy wysyła wiadomość, aby powiedzieć, że nie może znaleźć twojego domu.

**JAK:**
Wiadomość przychodząca za pośrednictwem wiadomości tekstowej lub e-mail od dużej firmy kurierskiej informuje, że kierowca nie był w stanie dostarczyć paczki do miejsca zamieszkania. Często wiadomość zawiera link twierdzący, że zapewnia informacje o śledzeniu. Link ten prawdopodobnie prowadzi do infostealera, który wyssie twoje dane uwierzytelniające.

**PRZYGOTUJ SIĘ:**
Firmy kurierskie są świadome tego typu oszustw. W rezultacie prawdopodobnie nigdy nie skontaktują się z Tobą przez e-mail lub SMS, aby poinformować Cię o nieudanej dostawie, zwłaszcza w okresie świątecznym. Możesz bezpiecznie zignorować wszystkie te wiadomości. Jeśli nie możesz oprzeć się chęci dowiedzenia się więcej na temat dostawy, którą miałeś otrzymać, skontaktuj się z nadawcą bez klikania w jakikolwiek przesłany link.


# Naruszenie, które ma znaczenie

## LinkedIn

**DLACZEGO MA TO ZNACZENIE::**
LinkedIn to jedyna duża sieć społecznościowa, która istnieje od dwóch dekad i pozostaje kluczową platformą dla osób fizycznych i firm na całym świecie. W listopadzie 2022 r. przestępcy twierdzili, że posiadają dane osobowe pół miliarda użytkowników serwisu i udostępnili 2 miliony rekordów jako dowód. Potwierdzono prawie 15 milionów skradzionych rekordów.

**NARUSZONE DANE:**
Dane te obejmują adresy e-mail, nazwy użytkowników, numery telefonów i inne dane osobowe, które mogą być wykorzystane do identyfikacji lub kierowania reklam do członków witryny.

**CO NALEŻY ZROBIĆ:**
Aktywni użytkownicy LinkedIn zazwyczaj otrzymują wiele wiadomości e-mail z serwisu tygodniowo, jeśli nie codziennie. Na razie wszyscy powinni unikać wszystkich wiadomości e-mail twierdzących, że pochodzą z witryny i odmawiać klikania jakichkolwiek linków w tych wiadomościach. Przejdź bezpośrednio do witryny, aby śledzić wszelkie otrzymane powiadomienia e-mail.

**Czy Twoje dane zostały ujawnione online?**
Sprawdź za pomocą naszego narzędzia
**F-Secure Identity Theft Checker!**

PROGNOZA

# Małe firmy na celowniku

Grupy przestępcze będą coraz częściej sprzedawać dostęp do baz danych wykradanych z mniejszych firm. Cel pozostanie niezmiennny: aby atakujący mogli oszukiwać konsumentów.

**Ash Shatrieh**
Badacz ds. analizy zagrożeń
**Helsinki, Finlandia**

## porada experta

Należy uważać na fałszywe wiadomości nawet od znanych osób, ponieważ hakerzy często wykorzystują wiarygodne firmy jako przebranie do ataków phishingowych..

**“Dane konsumentów przechowywane przez małe i średnie firmy stały się gorącym towarem dla cyberprzestępców”.**

Przez większość ostatniej dekady duże pieniądze w cyberprzestępczości pochodziły z ataków ransomware na duże organizacje. Zagrożenie to nadal istnieje. Ale przestępcy skupią się obecnie na małych i średnich przedsiębiorstwach (SMB). Konsekwencje dla konsumentów będą ogromne.

## Cyberatak jako usługa

Wykorzystanie technologii Software-as-a-Service (SaaS) do podstawowych funkcji biznesowych nadal integruje małe i średnie przedsiębiorstwa z globalnym łańcuchem dostaw. A ponieważ każda luka w zabezpieczeniach potencjalnie oferuje atakującym drogę do innych organizacji w łańcuchu, przestępcy często wykorzystują słabsze środki bezpieczeństwa stosowane przez małe i średnie firmy .

Tymczasem czarny rynek cyberprzestępczości odzwierciedla innowacje w legalnych usługach. Cyberprzestępczość jako usługa sprawia, że kampanie są łatwiejsze i tańsze do przeprowadzenia..

Mniejsze firmy już teraz mają do czynienia z większą liczbą naruszeń niż ich większe odpowiedniki. Tendencja ta prawdopodobnie będzie się nasilać, ponieważ duże grupy cyberprzestępcze koncentrują się na sprzedaży zhakowanych dostępów atakującym, którzy następnie będą mogli w pełni wykorzystać skradzione dane do tworzenia hiper-spersonalizowanych oszustw, znacznie zwiększając wskaźnik powodzenia swoich programów. A to dopiero początek.

## Idealna reputacja do pozyskania

Atakujący mogą również wykorzystywać media społecznościowe lub konta e-mail zaatakowanych firm. Daje im to możliwość uzbrojenia się w ciężko wypracowaną wiarygodność firmy, tworząc idealną sekwencję oszustw, którą można wykorzystać do szerzenia dezinformacji lub kampanii cyberprzestępczych.

Na tym się prawdopodobnie na tym nie skończy. Strony internetowe od lat są infekowane w celu wyłudzania numerów kart kredytowych. Spodziewamy się jednak, że coraz więcej atakujących będzie osadzać inne złośliwe skrypty w witrynach SMB w celu wydobywania kryptowalut lub przekierowywania użytkowników do fałszywych aktualizacji. W rezultacie konsumenci mogą nieświadomie paść ofiarą oszustw.

# Sztuczna inteligencja Google sprawdza samą siebie

Bard pozwala teraz użytkownikom na “wygooglowanie” odpowiedzi chatbota, aby sprawdzić, czy nie zmyśla.

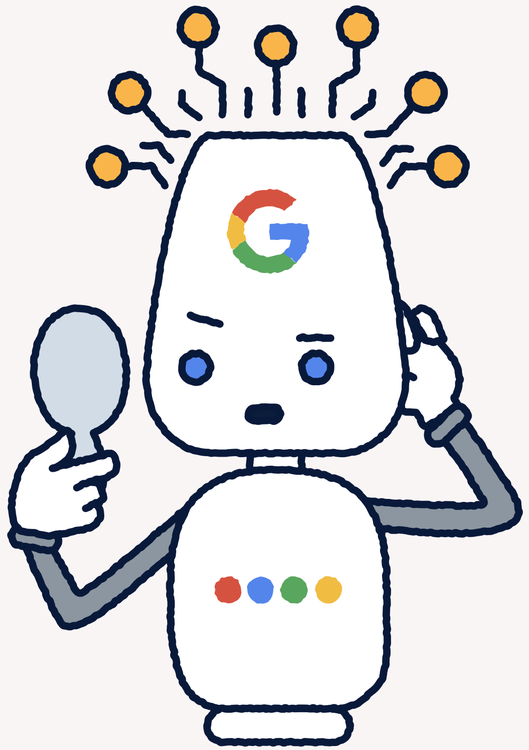
Jedną z najczęściej wymienianych obaw dotyczących chatbotów AI jest to, że generowane przez nie odpowiedzi mogą być "halucynacjami" i nie opierać się na faktach. Dwóch prawników z Nowego Jorku nauczyło się tej lekcji na własnej skórze, gdy zostali ukarani za złożenie briefu prawnego zawierającego cytaty z sześciu spraw, które zostały wymyślone przez ChatGPT.

Mając nadzieję na uniknięcie tego rodzaju nieporozumień, Google dodało nową funkcję do swojego “konwersacyjnego narzędzia AI” Bard, umożliwiając użytkownikom “podwójne sprawdzenie” faktów odpowiedzi AI za pomocą wyszukiwarki Google.

## Pętla sprzężenia zwrotnego złych informacji

“Modele generatywne, choć potężne i dość dokładne, nie są nieomylne” - powiedział Khalid Alnajjar, badacz danych o zagrożeniach w F-Secure. “Są one szkolone na ogromnych ilościach danych online, absorbując i powielając znalezione wzorce”.

Khalid zauważył, że problemy z treściami generowanymi przez sztuczną inteligencję mogą łatwo wzrosnąć, ponieważ “przyszłe wersje tych modeli mogą uczyć się więcej na podstawie własnych kreacji”. Dodatkowo, modele te będą nieuchronnie karmione szkodliwymi dezinformacjami rozpowszechnianymi przez ludzi.



“Może to stworzyć pętlę sprzężenia zwrotnego złych informacji, chyba że zostaną wdrożone mechanizmy zapobiegające temu”.

## Długa podróż

Khalid nazwał funkcję “Google it” Bard AI znaczącym postępem w tej dziedzinie, ale ostrzegł, że to dopiero początek długiej drogi do zapewnienia, że generatywna sztuczna inteligencja tworzy wiarygodny tekst.

“Sprawdzanie faktów odbywa się za pomocą wyszukiwarki Google, która sprawdza, czy to, co wygenerował system, jest prawdziwe, czy nie" - podsumował. "Takie podejście nie jest pozbawione problemów, ponieważ Bard AI może sprawdzać swoje wyniki pod kątem fałszywych wiadomości, czyi uwzględniać je w wynikach wyszukiwania”.

**Khalid Alnajjar**
Badacz danych o zagrożeniach
**Helsinki, Finlandia**

**porada experta**

Zawsze podchodź do treści generowanych przez sztuczną inteligencję z pewną dozą sceptycyzmu. Gdy sztuczna inteligencja podaje źródła na poparcie swoich twierdzeń, nie bierz ich za dobrą monetę - sprawdź ich wiarygodność.

**“Modele generatywne, choć potężne i dość dokładne, nie są nieomylne”.**

# OSZUSTWA na jedno złe KLIKNIĘCIE

**Cyberprzestępstwa, z którymi najprawdopodobniej będziesz mieć do czynienia, polegają na nakłonieniu cię do dokonania jednego złego wyboru.**

**Oszustwa to biznes wart biliony dolarów, którym spotyka się więcej niż 1 na 4 osoby na świecie*.**

Oszustwa są wielokanałowe, wyjaśnił Joel Latto, doradca ds. zagrożeń w F-Secure..

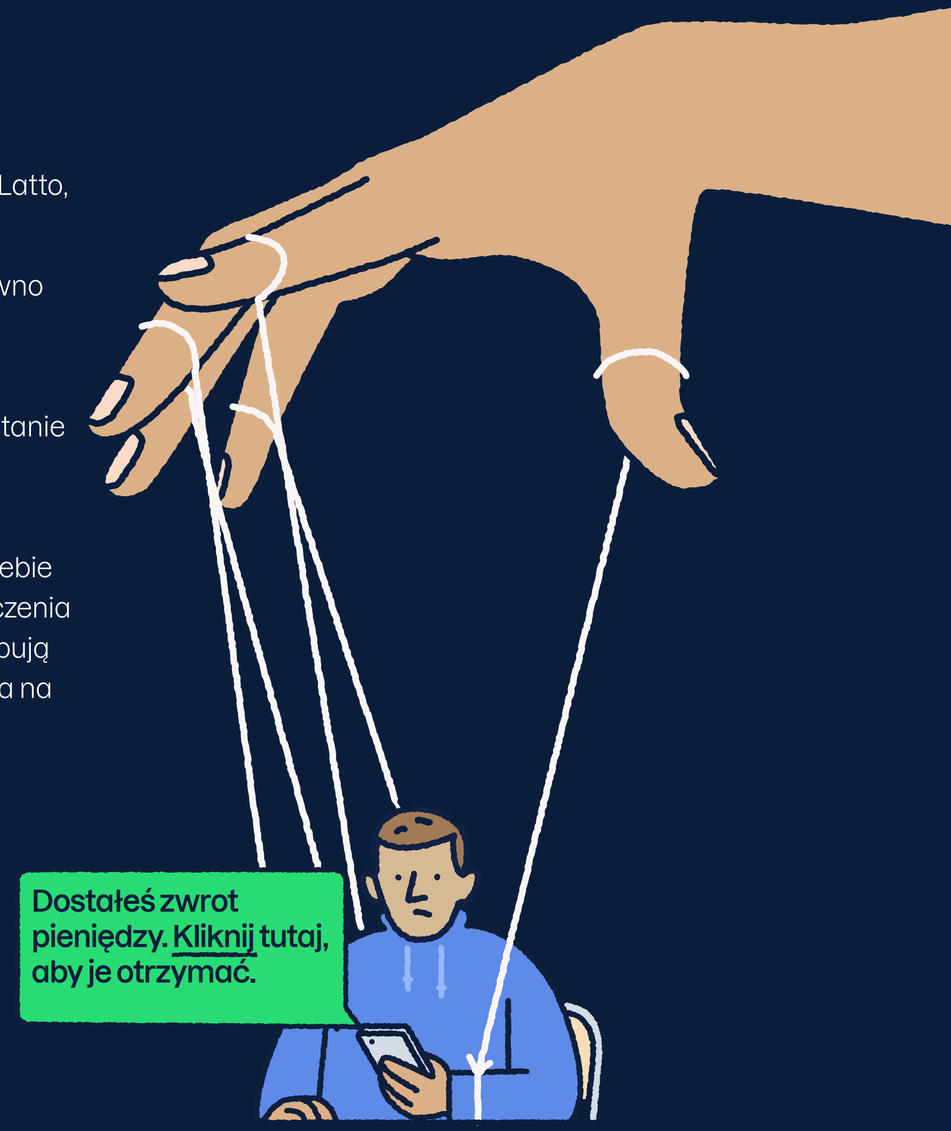
“Oznacza to, że mogą ci się przytrafić zarówno w Internecie, jak i poza nim” -powiedział.

Jeśli jednak padniesz dziś ofiarą cyberprzestępstwa, najprawdopodobniej stanie się to za pośrednictwem telefonu.

“I zamiast infekować cię złośliwym plikiem, przestępcy najprawdopodobniej dotrą do ciebie za pomocą wiadomości tekstowej lub połączenia telefonicznego” - powiedział. “I po prostu próbują znaleźć sposób, aby skłonić cię do spojrzenia na ekran i wykonania jednego złego kliknięcia”.

## Najczęstsze formy cyberprzestępczości**

| | |
|---|---|
| **12%** | Oszustwo SMS-owe |
| **11%** | Oszustwo telefoniczne |
| **8%** | Złośliwe oprogramowanie i wirusy |
| **6%** | Oszustwo z wykorzystaniem karty kredytowej |




*Źródło: Globalny stan oszustw - 2023 r., ScamAdviser ** Źródło: F-Secure Consumer Market Research, czerwiec 2023, 11 krajów (Brazylia, Finlandia, Francja, Niemcy, Włochy, Japonia, Holandia, Norwegia, Szwecja, Wielka Brytania i USA), n=4400

**Joel Latto**
Doradca ds. zagrożeń
**Helsinki, Finlandia**

**porada experta**

## "Każdy w końcu źle klika. Dlatego potrzebujesz wysokiej jakości rozwiązania zabezpieczającego, takiego jak F-Secure Total, a u naszych Partnerów wspólnie oferowana usługa ochrony w internecie, które obejmuje ochronę przeglądania".


## Trendy

### Black Friday Wyciekły akty z mistrzostw świata

Przestępcy wykorzystują dowolny popularny temat, aby przyciągnąć uwagę użytkownika.

A chatboty AI tylko ułatwiają lokalizowanie oszustw.

“Ostatnio zauważyłem przykłady jednego oszustwa na Facebooku w języku szwedzkim, węgierskim, francuskim i niemieckim, podczas gdy wcześniej widziałem je prawie wyłącznie w języku angielskim” - powiedział.

Złośliwe oprogramowanie to sposób, w jaki cyberprzestępcy dostają się do Twoich urządzeń. Oszustwa to sposób, w jaki dostają się do naszych umysłów. A oszukiwanie ludzi może być zarówno grą ilościową, jak i jakościową.

“Przykładem oszustwa na dużą skalę może być kampania spamowa z fałszywymi reklamami na Facebooku skierowanymi do dużej liczby odbiorców" - powiedział Joel. "Ale ukierunkowane oszustwo może być równie dużym zagrożeniem, a w takim przypadku przestępca może zbadać twoje życie online, zanim jeszcze się zacznie”.

PROGNOZA

# Sztuczna inteligencja będzie większa niż Internet

Każdy, kto zignoruje sztuczną inteligencję, spotka ten sam los, co tych, którzy zignorowali Internet.

**Mikko Hyppönen**
Główny doradca ds. badań
**Helsinki, Finlandia**

**porada experta**

Spróbuj przesłać długi plik PDF - w dowolnym języku - do Claude.ai lub ChatGPT i poproś o podsumowanie. Myślę, że będziesz pod wrażeniem. Wypróbowałem to z kilkoma napisanymi przeze mnie artykułami i z pewnością byłem pod wrażeniem.

**“Zostaniemy zapamiętani jako pierwsi ludzie, którzy mieli dostęp do sztucznej inteligencji”.**

Internet wymazał granice. Wywołał rewolucję tak transformacyjną, że napisałem w mojej książce *If It's Smart, It's Vulnerable*, która została opublikowana latem 2022 roku, że zostaniemy zapamiętani jako pierwsi ludzie, którzy weszli do sieci. Myliłem się.

Zostaniemy zapamiętani jako pierwsi ludzie, którzy mieli dostęp do sztucznej inteligencji.

## Trzy obroty jednocześnie

Internet był tylko pierwszą z trzech rewolucji, które miały miejsce mniej więcej w tym samym czasie, co doprowadziło nas do eksplozji sztucznej inteligencji, której obecnie doświadczamy.

Przeniesienie niemal każdej informacji do Internetu pomogło przekształcić całą zawartość, która istniała na papierze, w dane. Druga rewolucja była częścią pierwszej i dała nam możliwość przechowywania wszystkich tych danych. Nazywamy to “chmurą”. Trzecia rewolucja prawdopodobnie znajduje się teraz w Twojej kieszeni. Nie chodzi o sam telefon. To moc obliczeniowa, która w nim drzemie. Typowy smartfon z 2023 roku byłby jednym z 500 najlepszych superkomputerów na świecie zaledwie 20 lat temu.

W rezultacie możemy teraz nauczyć komputery tworzenia obrazów, które nie są ograniczone kreatywnością, i mamy duże modele językowe, które mogą mówić wszystkimi ludzkimi językami. W ciągu około dekady będziemy w stanie wybrać dowolnego aktora do roli w dowolnym filmie, który chcemy obejrzeć na Netflix. Ostatecznie sztuczna inteligencja może być również wykorzystywana do leczenia raka, rozwiązywania problemów związanych ze zmianami klimatu i przepisywania własnego kodu w celu ciągłego doskonalenia się.

## Drugi najbardziej inteligentny gatunek

Co to dla nas oznacza? Czy celowe uczynienie z siebie drugiego najbardziej inteligentnego gatunku na planecie jest mądrą decyzją? Jak istoty ludzkie, z naszą średnią inteligencją 100 IQ, mogą przewidywać, że nadludzkie SI z miliardowym IQ będą się zachowywać?

To, co możemy teraz zrobić, to zastanowić się, w jaki sposób sztuczna inteligencja może być wykorzystywana i niewłaściwie wykorzystywana. Ponieważ jeśli tego nie zrobimy, możemy być pewni, że zrobią to nasi konkurenci i oszuści, którzy mogą wykorzystać sztuczną inteligencję.

# Ekosystem Booking.com celem ataku

## Fałszywe potwierdzenia pokazują, jak trudno jest zabezpieczyć sieć milionów hoteli i prywatnych hostów.

Działaj szybko. Wyślij nam dane swojej karty kredytowej. W przeciwnym razie stracisz rezerwację.

Tak brzmiała wiadomość w e-mailach "potwierdzających" wysłanych niedawno do wielu klientów Booking.com. Firma zaprzeczyła włamaniu do swoich systemów i zasugerowała, że systemy hoteli partnerskich zostały naruszone. Jest to jednak niewielka pociecha dla klientów, którzy zostali poinformowani przez swoją firmę, że dane ich kart kredytowych mogły zostać naruszone.

### Zaufanie można wykorzystać

"Oszustwa związane z rezerwacjami nie są niczym nowym, ale stają się coraz bardziej zaawansowane" - powiedział Hoai Duc Nguyen, badacz ds. ochrony przed zagrożeniami w F-Secure. "Ale ten przykład pokazuje, jak trudno jest zabezpieczyć branżę, w której wiele platform wynajmuje pokoje zarówno od hoteli, jak i prywatnych właścicieli".

Booking.com to jedna z najpopularniejszych aplikacji turystycznych na świecie. Oferuje usługi rezerwacji noclegów dla prawie 3 milionów obiektów, w tym 2,3 miliona powiązanych prywatnych domów i apartamentów. Atakujący przeprowadzili te ataki, wykorzystując zaufanie między klientami a wiadomościami wysyłanymi przez platformę rezerwacyjną oraz strach klientów przed utratą planów podróży.

### Wysoki sezon dla oszustów

"Prywatni gospodarze są najbardziej narażeni na oszustwa i phishing, ponieważ nie są często szkoleni w zakresie cyberataków" - dodał Hoai Duc.

Badacze zidentyfikowali ataki phishingowe ukierunkowane na prywatnych gospodarzy i hotele współpracujące z Booking.com, które prowadzą do infekcji złośliwym oprogramowaniem infostealer, które wysysa dane klientów.

"Właściciele hoteli i gospodarze są pod ogromną presją w szczycie sezonu" - powiedział Hoai Duc. "Chociaż te oszustwa mogą wydawać się oczywiste, o wiele łatwiej jest dać się oszukać, gdy ma się do czynienia z setkami lub tysiącami rezerwacji".

**Hoai Duc Nguyen**
Badacz ds. ochrony przed zagrożeniami
**Helsinki, Finlandia**

**porada experta**

Zastanów się dwa razy, gdy otrzymasz nieoczekiwaną wiadomość z silnymi emocjami, ostrzeżeniem, w które zaangażowane są pieniądze - nawet jeśli wiadomość ta pochodzi od zaufanego partnera..

**"Oszustwa związane z rezerwacjami nie są niczym nowym, ale stają się coraz bardziej zaawansowane".**

PROGNOZA

# Sztuczna inteligencja zwiększy skalę oszustw zakupowych

Fałszywe reklamy promujące luksusowe produkty osiągną nowy poziom dzięki obrazom i tekstom generowanym przez sztuczną inteligencję.

**Yik Han**
Badacz
**Kuala Lumpur, Malaysia**

## porada experta

Przesyłając dane karty kredytowej, upewnij się, że procesor płatności jest legalny. Zapoznaj się z popularnymi stronami płatności, takimi jak Amazon, Shopify i Stripe.

**“Generatywne narzędzia sztucznej inteligencji pomogą oszustom tworzyć bardziej przekonujące podpisy i szokująco szczegółowe obrazy”.**

W tym roku nastąpił gwałtowny wzrost liczby oszustw zakupowych dokonywanych za pośrednictwem fałszywych i oszukańczych reklam towarów luksusowych w mediach społecznościowych, głównie na Facebooku, Instagramie i Tik Tok. W 2024 r. te złe reklamy prawdopodobnie osiągną nowy poziom dzięki wykorzystaniu szybko rozwijającej się sztucznej inteligencji generatywnej (AI).

## Inteligencja sztuczna, oszustwa prawdziwe

Miliardy ludzi na całym świecie używają chatbotów AI do generowania tekstu i obrazów od czasu premiery ChatGPT, która wprowadziła tę technologię do głównego nurtu pod koniec 2022 roku. Postępy w generatywnej sztucznej inteligencji są trwałe i rozległe, ponieważ gigantyczni konkurenci technologiczni, w tym Google i Microsoft, szukają przewagi w tej szybko rozwijającej się przestrzeni.

I chociaż boty te automatyzują wiele zadań, są również często wykorzystywane w niewłaściwy sposób. W kwietniu 2023 r., Europol zauważył, że duże modele językowe (LLM), takie jak ten, który zasila ChatGPT, mogą być wykorzystywane przez przestępców do oszustw, dezinformacji i cyberprzestępczości, zauważając w szczególności, że LLM są “niezwykle przydatnym narzędziem do celów phishingowych”.


## Liczne zalety, ale nie doskonałość

Generatywne narzędzia sztucznej inteligencji pomogą oszustom tworzyć bardziej przekonujące podpisy i szokująco szczegółowe obrazy w ich fałszywych reklamach. Firma F-Secure zaobserwowała już wzrost wykorzystania narzędzi generatywnej sztucznej inteligencji zarówno w legalnych, jak i nielegalnych postach reklamowych w mediach społecznościowych.

Cyberprzestępcy prawdopodobnie będą również tworzyć więcej fałszywych witryn zakupowych i łączyć je ze złośliwymi reklamami, aby nakłonić ofiary do podania numerów kart kredytowych. Z pomocą generatywnej sztucznej inteligencji, która natychmiast wspomaga tworzenie całych doświadczeń e-commerce i pomaga w tworzeniu profesjonalnych komunikatów marketingowych, te oszukańcze witryny staną się jeszcze trudniejsze do wykrycia.

# Nagrody F-Secure

## za doskonałość w ochronie cyfrowych chwil

Zabezpieczenie każdej cyfrowej chwili to wysiłek zespołowy. Dlatego wraz z końcem 2023 roku chcieliśmy uhonorować przełomowe odkrycia w dziedzinie cyberbezpieczeństwa, które w tym roku uczyniły nas wszystkich nieco bezpieczniejszymi.

### Najlepsza innowacja w dziedzinie bezpieczeństwa: Passkeys

Apple, Amazon i Microsoft wdrożyły tę nową metodę uwierzytelniania. Tegoroczna jesień przyniosła jednak przełom w tej technologii, która ma być szybka, bezpieczna i łatwa do zapamiętania. Google wprowadziło domyślne klucze dostępu na wszystkich kontach osobistych. Powinno to oznaczać, że śmierć haseł jest nieuchronna. I dobrze.

### Najlepszy obalenie: Genesis Market

Liczby są ogromne. Organy ścigania z 17 krajów dokonały 119 aresztowań. Naruszono bezpieczeństwo ponad 1,5 miliona komputerów. Ponad 80 milionów danych uwierzytelniających konta na sprzedaż. Zlikwidowanie Genesis Market w kwietniu ustanowiło nowy standard współpracy międzynarodowej w celu zamknięcia rynku sprzedającego skradzione dane uwierzytelniające. Dobra robota.

### Najlepsza ochrona przed oszustwami: Weryfikacja Google

Google nazywa to BIMI, Brand Indicators for Message Identification. Istnieje od 2021 roku, ale w tym roku firma dodała niebieski znacznik wyboru w Gmailu, który wskazuje, że wiadomość e-mail pochodzi od firmy, która twierdzi, że ją wysłała. Nie wyeliminuje to wszystkich oszustw phishingowych. Ale powinno pomóc.

### Najlepsza niezamierzona konsekwencja: X pobiera opłaty za SMS 2FA

X (dawniej Twitter) ogłosił w lutym, że będzie pobierał opłaty za uwierzytelnianie dwuskładnikowe (2FA) za pomocą wiadomości SMS. Chociaż posunięcie to osłabiłoby bezpieczeństwo konta tych, którzy wyłączyli tę funkcję, zmusiłoby to również użytkowników do przyjęcia bezpłatnej aplikacji uwierzytelniającej, która jest bezpieczniejszą opcją blokowania konta. Jeśli jeszcze tego nie zrobiłeś, porzuć wszystkie kody SMS 2FA i korzystaj z aplikacji!

### Najlepsze proste rozwiązanie: Online Shopping Checker

Dzięki nowoczesnym narzędziom internetowym i sztucznej inteligencji stworzenie legalnego sklepu internetowego zajmuje tylko kilka minut. Dlaczego więc przestępcy nie mieliby założyć fałszywego sklepu i czerpać z tego korzyści? Konsumenci mają wreszcie sposób na łatwe sprawdzenie, czy sklepy, na które trafili, są legalne. Online Shopping Checker natychmiast sprawdza reputację sklepu za darmo. Ta sama technologia jest teraz dostępna w produkcie F-Secure Total's Browsing Protection. Wypróbuj!

# Bezpieczeństwo w internecie z F-Secure

- Ochrona kont bankowych i płatności w sieci
- Ochrona antywyłudzeniowa, która blokuje wejścia na fałszywe strony
- Blokowanie podrobionych aplikacji, które mogą służyć do wykradania danych
- Limit czasu przed ekranem i pora spać, aby dzieci zdrowo korzystały z telefonów

# Ochrona tożsamości od F-Secure

- Monitorowanie wycieków danych do internetu
- Natychmiastowe alerty z poradami krok po kroku co zrobić w kryzysowej sytuacji
- Pomoc w tworzeniu mocnych i unikalnych haseł

F-Secure