Jak wybrać bezpieczną pocztę e-mail? Usługi i programy

Gmail, Proton Mail, a może inna usługa poczty elektronicznej – sprawdź, która poczta jest najbardziej bezpieczna oraz dba o prywatność użytkowników i chroni ich e-maile.

Znalezienie najbezpieczniejszej poczty e-mail może być trudnym zadaniem. Ten przewodnik zawiera **wszystkie niezbędne informacje**, które pomogą Ci wybrać bezpieczną pocztę elektroniczną.

Omówimy przede wszystkim kwestie dotyczące bezpieczeństwa, **poznasz również zasady**, które ułatwią Ci świadomy wybór poczty e-mail (dowiesz się nawet jak stworzyć własną testową kampanię phishingową). Na koniec przyjrzymy się niektórym z **najlepszych opcji dostępnych na rynku**, jeśli chodzi o bezpieczne wiadomości e-mail.

Spis treści

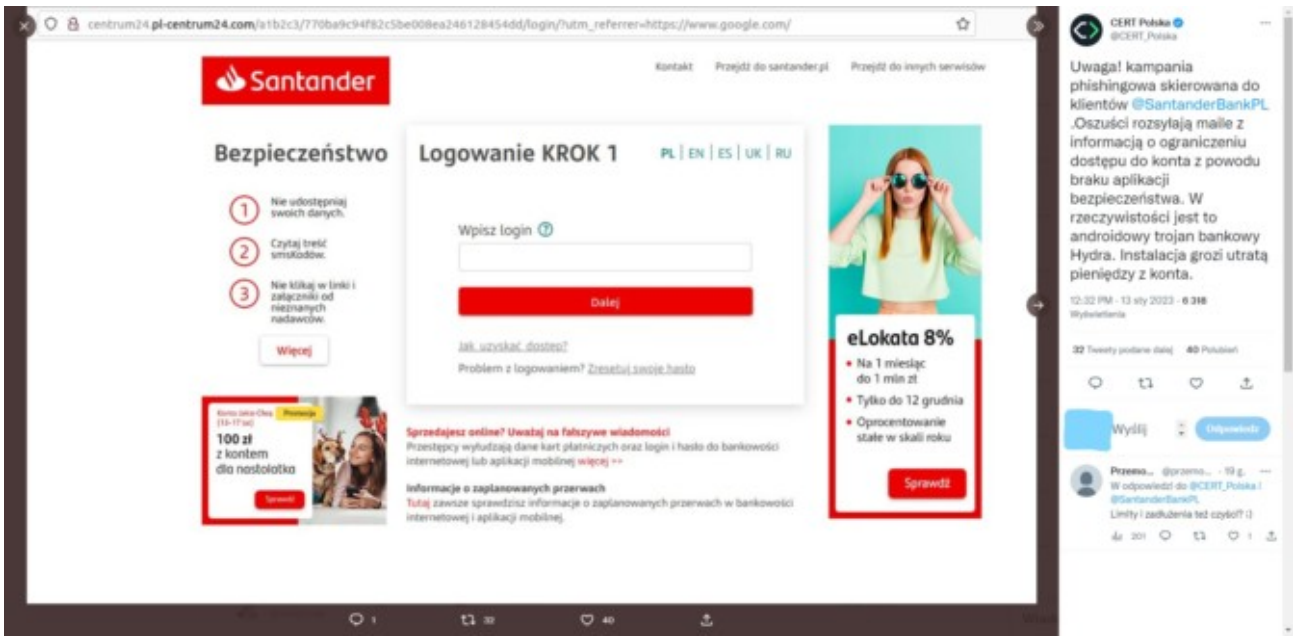
- Jaka alternatywa dla Gmail?
- Gdzie najlepiej założyć konto pocztowe?

Bezpieczna poczta elektroniczna – którą wybrać?

Dlaczego powinieneś przemyśleć z jakiej poczty elektronicznej korzystać? To kwestia **bezpieczeństwa przesyłanych informacji**, a z drugiej strony **prywatności Twojej korespondencji**.

Ataki z użyciem poczty elektronicznej

E-mail stał się **ulubionym narzędziem cyberprzestępców**. 94 proc. złośliwego oprogramowania rozprzestrzenia się pocztą elektroniczną (raport PhishingBox z 2019 roku).



Wiadomości służą m.in. do groźnych ataków ransomware, czyli z użyciem **oprogramowania szantażującego**.

Atak przebiega następująco. Dostajesz na prywatną lub firmową skrzynkę odbiorczą e-mail z załącznikiem. To często wyglądający niegroźnie dokument – w 2020 roku źródłem ok. 41 proc. skutecznych ataków były **dokumenty pakietu Office**.

Po otwarciu załącznika ukryty w nim ransomware szyfruje pliki na dysku w Twoim komputerze. Dostajesz też informację, że musisz **zapłacić okup** (w kryptowalutach), aby odzyskać dostęp do danych. Wiele firm płaci przestępcom, jednak nie ma pewności, że agresor dotrzyma słowa. Czasem pliki są nieodwracalnie zniszczone.

To nie wszystko. Gangi ransomware stosują **podwójny szantaż**. Żądają pieniędzy za nieujawnianie danych, które zaszyfrowali. Dla wielu firm to ogromny problem – po wycieku poufnych informacji stracą reputację, klientów oraz narażą się na konsekwencje prawne.

Pamiętaj, że Twój bezpieczny mail jest ważny również dla innych osób. **Przestępcy użyją przejętą skrzynkę pocztową** i wyślą z niej złośliwe wiadomości e-mail na adresy z bazy kontaktów. Twoi znajomi mogą paść ich ofiarą – stracić pieniądze lub wrażliwe dane.

Kto widzi treści wiadomości?

Dość często e-maile zawierają osobiste zdjęcia i filmy lub poufne dokumenty firmowe. Większość z nas jest przyzwyczajona do tajemnicy tradycyjnej korespondencji jednak w świecie cyber zasady są inne.

Pamiętaj, że cały czas, ktoś może zaglądać przez Twoje ramię i **obserwować, co wysyłasz pocztą e-mail.**

„Wiemy, że dostawcy usług internetowych i państwa mają możliwość i motywację do obserwowania ruchu w Internecie. Po drugie, dostawcy usług poczty elektronicznej stanowią **znacznie większe zagrożenie dla prywatności poczty** elektronicznej niż przypadkowi nieznajomi. Z nielicznymi wyjątkami dostawcy ci mogą czytać nasze wiadomości e-mail. Dotyczy to Google i Microsoft oraz organizacji, dla których pracujemy” – podkreślają autorzy książki „Cybersecurity myths and misconceptions”.

Jaka usługa e-mail jest bezpieczna, a jaką wybrać jeżeli zależy Ci przede wszystkim na prywatności? A może jest idealna poczta elektroniczna, która łączy obie cechy? Za chwilę znajdziesz odpowiedzi na te pytania.

Jaka jest bezpieczna poczta elektroniczna?

Zanim zobaczysz, która poczta elektroniczna jest najbardziej bezpieczna, spójrz na **ranking najpopularniejszych usług poczty elektronicznej** w Polsce (Gemius/PBI 2020):

- Gmail – 11 496 335 użytkowników,
- Wp.pl – 7 702 914,
- Onet.pl – 3 677 040,

- Interia.pl – 3 252 823,
- o2.pl – 3 048 168,
- Gazeta.pl – 302 533.

Poczta Yahoo, bardzo popularna w Stanach Zjednoczonych, w Polsce zajmuje dopiero 7 miejsce (choć jest darmowa i całkiem szczodra dla użytkowników – jej skrzynka odbiorcza pomieści aż 1 TB danych).

To popularność, a jak jest z bezpieczeństwem? Dyskusje na ten temat można prowadzić do rana, jednak większość ekspertów zgadza się, że pierwsze miejsce zajmuje poczta Gmail, czyli usługa Google. Dlaczego?

Bezpieczna darmowa poczta – Gmail

Gmail jest bardzo bezpieczną skrzynką pocztową, ponieważ Google stosuje wiele różnych metod, aby chronić Twoje dane. To m.in. szyfrowanie połączeń, automatyczne skanowanie poczty w celu wykrycia spamu i złośliwego oprogramowania, a także uwierzytelnianie dwuskładnikowe, które wymaga podania hasła i jednorazowego kodu dostarczonego przez aplikację na telefonie, aby uzyskać dostęp do konta (możesz też skorzystać z fizycznego klucza bezpieczeństwa).

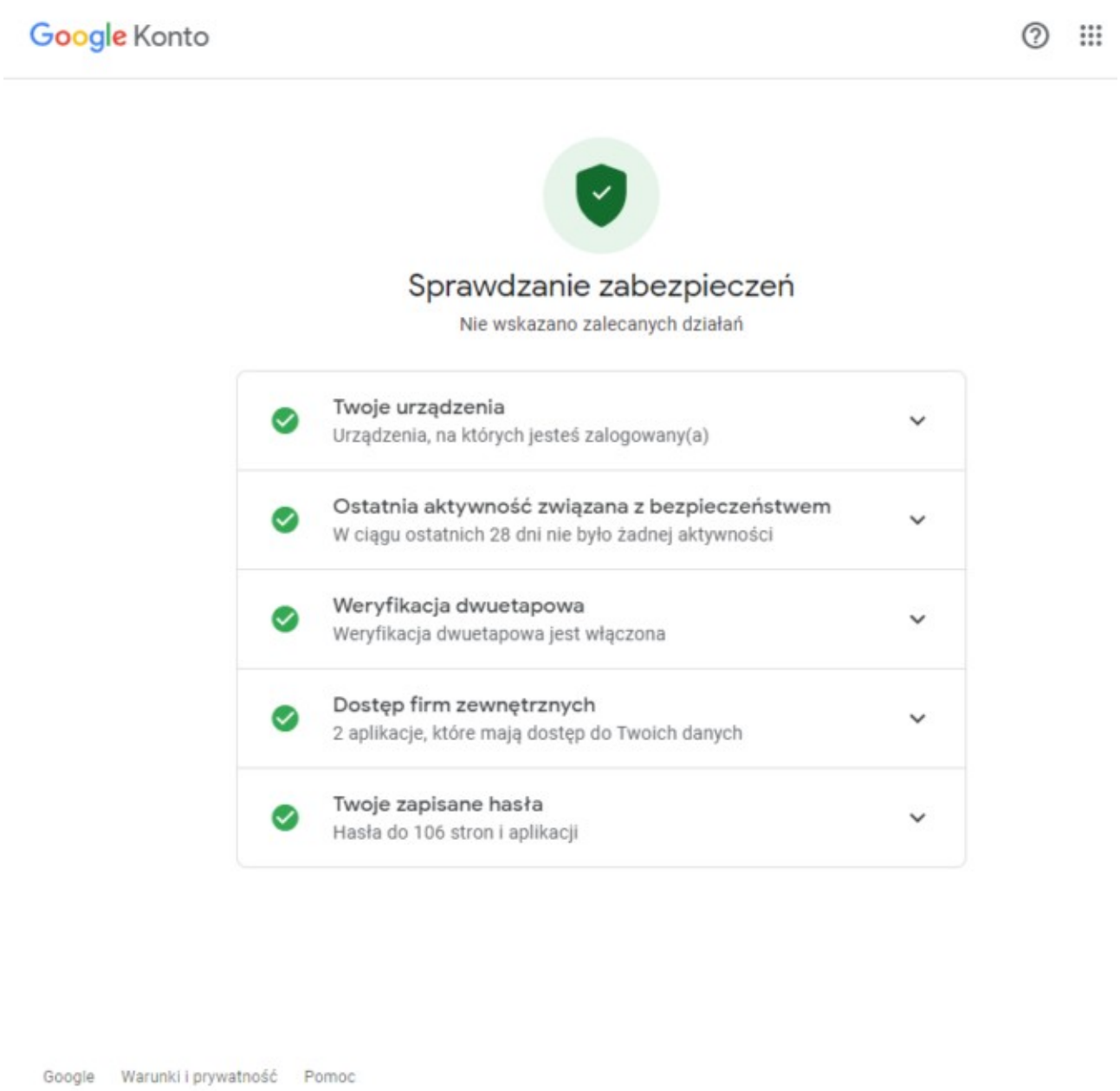
Spójrz na szczegóły. Oto powody, dla których poczta Gmail jest prawdopodobniej najbezpieczniejsza:

- nad bezpieczeństwem usługi czuwa **rozbudowany zespół ekspertów**, który sprawnie reaguje na zgłoszenia od użytkowników,
- wiadomości e-mail są **skanowane w poszukiwaniu spamu, złośliwego oprogramowania** lub treści niezgodnych z prawem (np. pornografii dziecięcej),

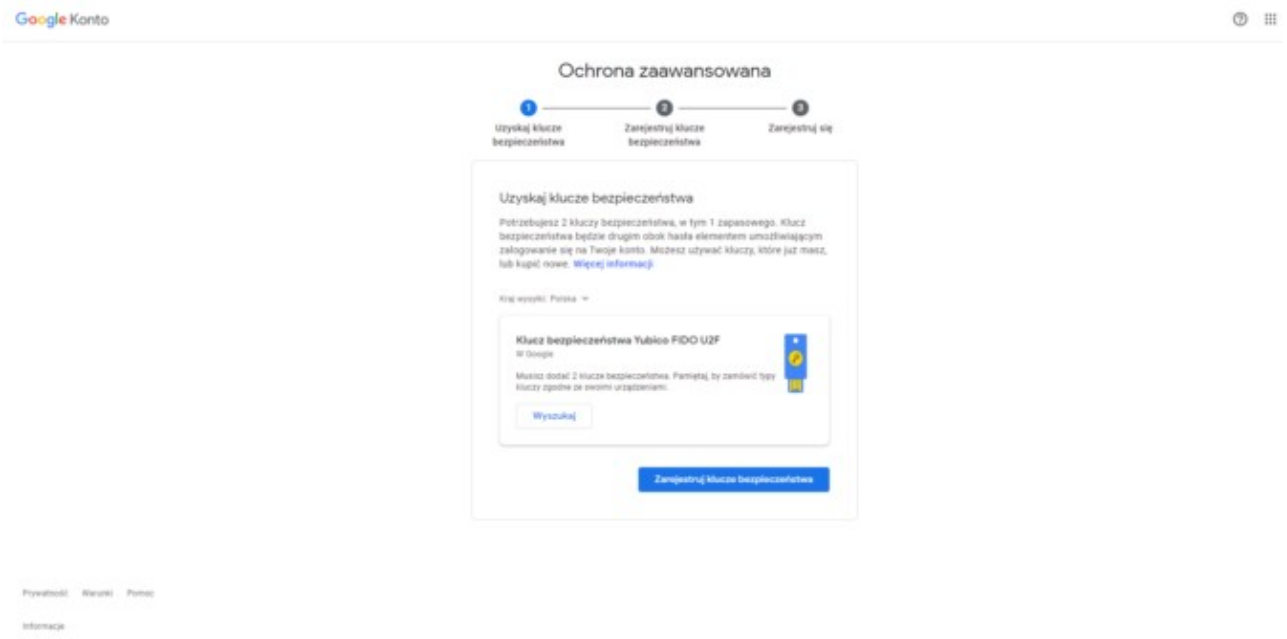
- ma bardzo dobre **zabezpieczenia przed spamem**, a jej filtry świetnie powstrzymują kampanie spamowe,
- poczta Gmail **ostrzega przed niebezpiecznymi e-mailami**, co ułatwia po stronie klienta ochronę przed atakami,
- ze względu na potężną liczbę użytkowników i obsługiwanych maili, fachowcy Google potrafią **szybko i trafnie zidentyfikować próby cyberataków**,
- możesz sam **zdecydować o poprawie bezpieczeństwa swojej skrzynki pocztowej** w Gmail – wystarczy wejść na Konto Google (kliknąć w swoje zdjęcie) >Zarządzaj kontem i wybrać odpowiednie ustawienia, np. włączyć weryfikację dwuetapową (zalecam, przy użyciu fizycznego klucza bezpieczeństwa, który daje w praktyce niemal 100 proc. ochronę przed phishingiem)
- dodatkowych zabezpieczeniem – przede wszystkim dla osób, które pracują z wrażliwymi/poufnymi informacjami – jest włączenie **Ochrony zaawansowanej** (potrzebujesz do niej dwóch kluczy bezpieczeństwa).
- Google oferuje **pieniądze dla osób, które znajdą podatności w jego usługach** (programu bug bounty) – firma proponuje 100 – 13 337 dolarów dla znalazcy. W 2021 r. wypłaciła w sumie ponad 6 mln USD.

		Impact [1]		
		High	**Medium**	**Low**
Probability [2]	**High**	Up to $13,337	$3,133.7 to $5,000	$1,337
	Medium	$3,133.7 to $5,000	$1,337	$100 to $500
	Low	$1,337	$100 to $500	HoF Credit

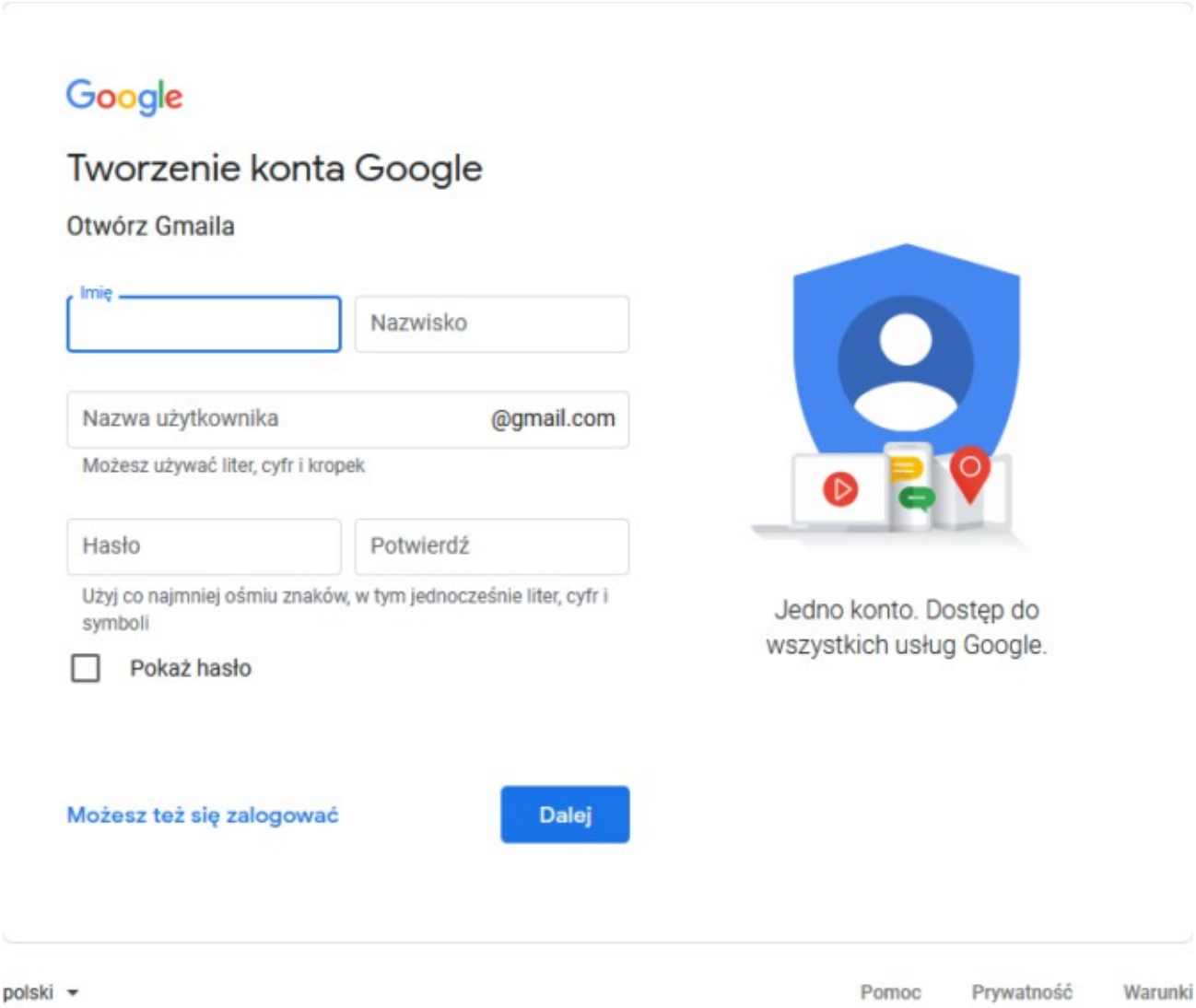
Poczta Gmail jest bezpieczna, bo duży może więcej.



Z pewnością Google przyciąga użytkowników potrzebujących więcej miejsca na dysku – skrzynka odbiorcza wraz z dokumentami na Google Drive pomieści 15 GB (za 100 GB zapłacisz 8,99 zł miesięcznie) – wygodnego interfejsu oraz niezawodnego działania.



Jaka jest największa wada poczty Gmail? Zarzuty dotyczą przede wszystkim **kwestii prywatności**.



Zakładając darmowe konto Google (potrzebne do korzystania z Gmaila) podajesz dużo prywatnych informacji. To nie wszystko.

Gmail to tylko pozornie darmowa poczta. Google wykorzystuje skrypty śledzące, które obserwują każdy nasz ruch, a **zdobyte informacje są towarem**.

W warunkach korzystania z usług Google czytamy, że firma ta używa „automatycznych systemów i algorytmów do **analizowania treści użytkownika**” pod kątem spamu, złośliwego oprogramowania, treści niezgodnych z prawem oraz dostosować usługi do użytkownika (np. spersonalizować wyniki wyszukiwania oraz reklamy).

Chcesz uciec spod lupy cyfrowego potentata? W praktyce **bardzo trudno uniknąć skanowania wiadomości** e-mail przez Google. Jak zauważa serwis Zaufana Trzecia Strona, *„jeśli nie korzystasz z Gmaila i myślisz, że dzięki temu Google nie przeskanuje Twojej korespondencji, to się mocno łudzisz, bo wielu Twoich znajomych Gmaila pewnie używa”*.

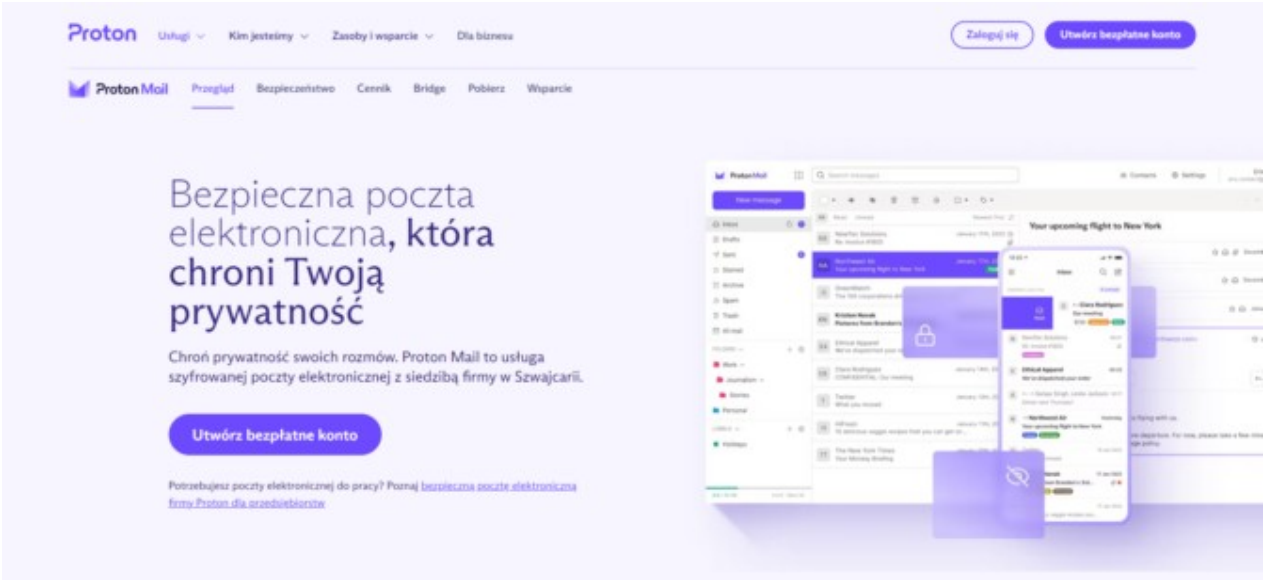
Choć nie odpowiadasz za pocztę, której używają znajomi i współpracownicy, to sam możesz założyć skrzynkę pocztową na serwisie, który zapewnia **wysoki poziom prywatności.**

Jaka prywatna poczta e-mail?

Jak już wiesz, Gmail nie jest optymalnym rozwiązaniem jeżeli zależy Ci na ochronie prywatności. Na szczęście dostępne są usługi poczty elektronicznej firm, których z zasady **nie interesuje o czym piszesz w swoich wiadomościach**.

Do najbardziej cenionych należy **Proton Mail**, firma z siedzibą w Szwajcarii założona w 2014 roku przez pracowników ośrodka naukowo-badawczego CERN.

Prywatne e maile – Proton Mail



Proton Mail to usługa poczty elektronicznej stawiająca na piedestale prywatność użytkowników potrzebujących dodatkowych zabezpieczeń.

To **darmowa poczta z możliwością płatnej subskrypcji**. Spójrz na zalety Proton Mail:

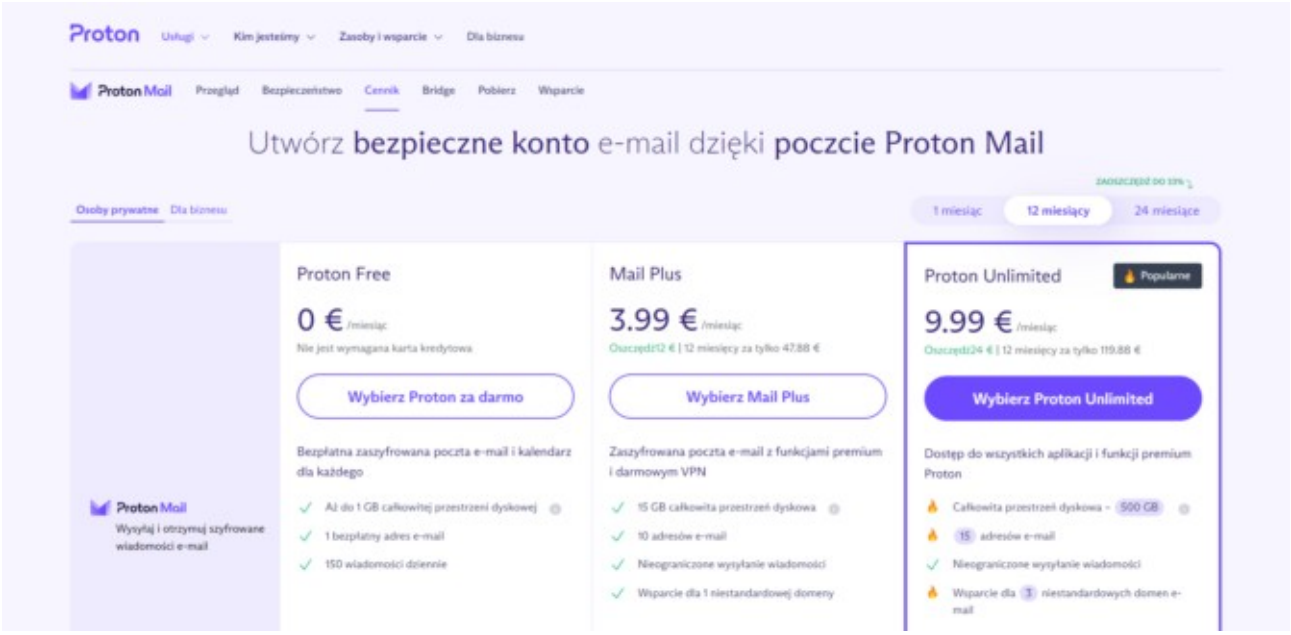
- oferuje **szyfrowanie komunikacji** po stronie klienta (dostawca maila nie widzi treści wiadomości e mail) z użyciem najwyższego standardu kryptograficznego 256-bitowy AES,
- zawartość skrzynki pocztowej użytkowników Proton Mail nie jest dostępna dla żadnych osób trzecich, nawet pracowników firmy, **tylko Ty możesz czytać swoje e-maile**,
- szyfrowanie wiadomości wychodzących ze skrzynki pocztowej jest automatyczne i nie wymaga żadnych umiejętności technicznych ani oprogramowania,
- możesz zaszyfrować wiadomość wysyłaną do odbiorcy, **który nie używa Proton Mail** – wybierasz hasło, z którego skorzysta tylko adresat,
- możesz zabezpieczyć dostęp do swojej skrzynki odbiorczej przy użyciu 2FA, czyli **uwierzytelnienia dwuskładnikowego** z użyciem fizycznych kluczy bezpieczeństwa (nie ma lepszego zabezpieczenia przeciwko phishingowi),
- ochrona wychodzących i przychodzących wiadomości **przed śledzeniem przez reklamodawców** (nie musisz martwić się, że Twoje dane są na sprzedaż i posłużą np. do profilowania reklam),
- serwery Proton Mail znajdują się w Szwajcarii, kraju, który ma bardzo **restrykcyjne przepisy dotyczące prywatności** (choć nie chroni to użytkowników poczty przed działaniem policji, także międzynarodowego Europolu),
- możesz go używać z **popularnymi klientami poczty** e-mail (np. Microsoft Outlook, Apple Mail, Mozilla Thunderbird) – za pomocą Proton Mail Bridge zaszyfrujesz swoje wiadomości e mail. To usługa dla płatnych subskrybentów,
- Proton Mail ma **otwarty kod źródłowy** – każdy (z odpowiednią wiedzą i umiejętnościami) może sprawdzić jakość usługi poczty elektronicznej (firma poddaje się niezależnym audytom).

Z pewnością szyfrowanie wiadomości e-mail po stronie klienta jest największą zaletą usługi Proton. Jednak ta poczta elektroniczna ma też swoje ograniczenia.

Choć Proton Mail działa również jako darmowa poczta, to wszystkie jego zalety docenisz dopiero **po wykupieniu płatnego planu.**

Za darmo otrzymasz tylko **500 MB przestrzeni** dyskowej na skrzynkę odbiorczą (z opcją przesyłania załączników do 25 MB).

To nie wszystko. Jeżeli wysyłasz wiadomość e-mail do osoby, która nie korzysta z Proton, to T**wój adres i tytuł wiadomości nie jest szyfrowany**, podobnie lista kontaktów i adres IP użytkowników.



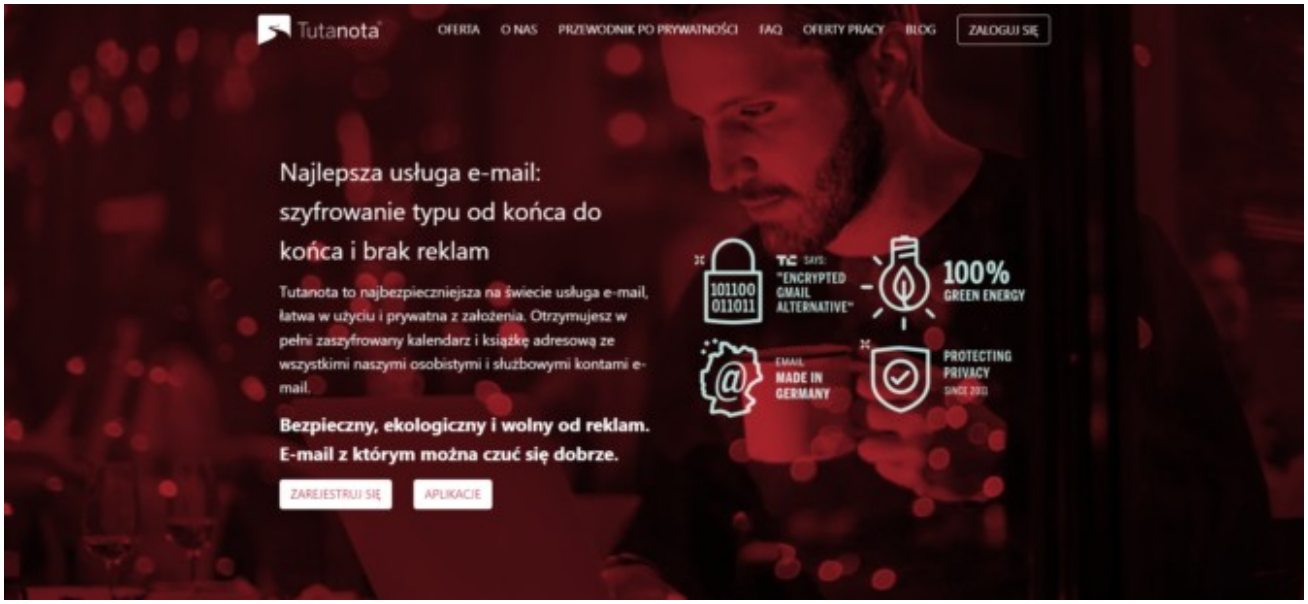
Zobacz moją pełną recenzję i opinie o Proton Mail.

Jaka jest inna skrzynka mailowa dbająca o prywatność?

Poczta Gmail nie odpowiada Ci, a nie chcesz też korzystać z Proton Mail?

Oto lista innych usług poczty elektronicznej, które **szanują prywatne dane swoich użytkowników** (za serwisem Privacy Tools):

- **Tutanota** – bezpłatna usługa open source poczty elektronicznej, która szyfruje wszystkie dane, z jednym adresem e-mail, kalendarzem oraz 1 GB przestrzeni dyskowej na skrzynkę odbiorczą, możliwe jest również korzystanie z płatnego konta obejmującego m.in. własną domenę, 5 dodatkowych adresów e-mail, wsparcie techniczne (płatne plany za 1 euro miesięcznie lub 4 euro dla rodziny), serwis umożliwia korzystanie z szyfrowania mail end-to-end lub wysyłanie niezaszyfrowanych wiadomości, dostępne bezpieczne konto biznesowe oraz konto rodzinne.
- **SimpleLogin** – usługa open source, która ukrywa prawdziwy adres użytkownika, wiadomości e mail przekazywane są do Twojej skrzynki pocztowej, a jeżeli odpowiesz, to odbiorca zobaczy alias. W darmowym planie jest m.in. 10 aliasów, w cenie 30 dolarów/rok lub 3 dolary/miesięcznie dodatkowe funkcje m.in. szyfrowanie komunikacji przy użyciu PGP,
- **mailbox.org** – płatna usługa poczty elektronicznej, cena 1,3 lub 9 euro miesięcznie (możliwy 30 dniowy bezpłatny test). W najtańszej subskrypcji m.in. 2 GB przestrzeni dyskowej na skrzynkę odbiorczą, w droższych 10-25 GB, 3-25 aliasów, kalendarz lub narzędzia do prowadzenia biura online. Plany biznesowe: 3-9 euro za jeden inbox i miesiąc,
- **StartMail** – płatna szyfrowana poczta elektroniczna, za 3 dolary miesięcznie (płatność roczna) otrzymujesz 10 GB przestrzeni dyskowej na maile, nielimitowane aliasy z domeną StartMail, dostęp z każdego urządzenia, za 3,50 dolarów miesięcznie dodatkowo dostajesz adres email oraz nielimitowane aliasy ze swoją domeną.



Możesz również korzystać z klienta poczty elektronicznej (programu służącego do wysyłania i odbierania e-maili), Privacy Tools poleca:

- **Thunderbird** (na komputer stacjonarny) – takie rozwiązanie docenią przede wszystkim zaawansowani użytkownicy, którzy nie lubią poczty w przeglądarce,
- **Mailvelope** (przeglądarka) – wtyczka do Chrome, Firefox i Edge, która szyfruje wysyłane e-maile używając PGP (szyfrowanie typu end-to-end), nie musisz zmieniać dostawcy swoich usług pocztowych, program kompatybilny z m.in. Gmail i Yahoo, treść wiadomości nie jest dostępna dla dostawców poczty email,

- **Canary Mail** (na iOS/Android) – szyfrowanie end-to-end, biometryczna blokada aplikacji, brak reklam, wykorzystuje sztuczną inteligencję (AI) do zarządzania zawartością poczty i wysyłania e-maili, usługa dostępna również na komputery Mac, plany: darmowy, Pro za 20 dolarów/rocznie oraz dla Enterprise za 10 dolarów/użytkownika/miesięcznie,
- **K-9 Mail** (na Android) – narzędzie typu open source, bardzo dobre do przeglądania dużej liczby wiadomości e mail.

Bezpieczny e-mail – 9 zasad wyboru programu pocztowego

Poczta e-mail jest podstawowym narzędziem komunikacji, ale może też stanowić zagrożenie dla Twojego cyber bezpieczeństwa. Ważne jest, abyś wybrał odpowiedni program pocztowy i przestrzegał zasad, aby mieć pewność, że poczta jest bezpieczna.

Oto **9 zasad wyboru bezpiecznej poczty e-mail**, które powinny pomóc Ci chronić siebie i swoje dane. Postępując zgodnie z tymi wskazówkami, będziesz mieć pewność, że Twoje e-maile są bezpieczne przed hakerami i innymi złośliwymi podmiotami.

1. **Uwierzytelnianie dwuskładnikowe** – zdecyduj się na usługę, która oferuje uwierzytelnianie dwuskładnikowe (2FA). To najlepszy sposób, żeby uniknąć włamania na konto i ataku phishingu. Najskuteczniejszą weryfikacją dwuetapową jest fizyczny klucz bezpieczeństwa, które używasz do logowania na kontach – nie można go podrobić lub podsłuchać.
2. **Szyfrowanie komunikacji end-to-end (E2EE)** – jeżeli zależy Ci na najwyższym poziomie bezpieczeństwa, to wybierz usługę z szyfrowaniem end-to-end: tylko Ty i odbiorca będziecie mieli dostęp do wiadomości.

3. **Dobra ochrona przed spamem** – wybierz usługę z dobrym filtrem spamu, aby zminimalizować ilość niechcianych wiadomości.
4. **Ochrona przed malware** – usługa poczty elektronicznej powinna mieć narzędzie do ochrony przed szkodnikami, które mogą dostać się do Twojej skrzynki odbiorczej, m.in. skanowanie antywirusowe, które wykryje i zablokuje złośliwe oprogramowanie oraz funkcje wykrywanie wiadomości phishingowych.
5. **Zabezpieczenia fizyczne** – sprawdź, na ile to możliwe, czy dostawca usługi przechowuje dane na bezpiecznych serwerach i posiada dobre procedury bezpieczeństwa hardware. Najbardziej renomowani usługodawcy informują użytkowników o stosowanych zabezpieczeniach.
6. **Polityka prywatności** – przeczytaj i zrozum politykę prywatności usługi, aby upewnić się, że właściciel usługi przetwarza dane zgodnie z Twoimi preferencjami (to szczególnie ważne w przypadku darmowej wersji e-maila).
7. **Lokalizacja** – zwróć uwagę na to, gdzie znajdują się serwery i czy dostawca podlega prawu, które chroni Twoją prywatność.
8. **Dostępność** – sprawdź, czy usługa e-mail jest stabilna i czy inni użytkownicy nie narzekają na długi czas przestojów.
9. **Wsparcie** – upewnij się, że dostawca oferuje dobre wsparcie techniczne, które pomoże Ci rozwiązać ewentualne problemy.

Wiesz już czym się kierować wybierając bezpieczny mail. Jednak nawet najlepsze zabezpieczenia nie powstrzymają wszystkich ataków.

Jesteś swoją pierwszą linią obrony – agresor nie musi tracić czasu i pieniędzy na przełamywanie zabezpieczeń skrzynki pocztowej. O wiele prościej rozesłać złośliwego e-maila i poczekać, aż ktoś go otworzy.

Jesteśmy tylko ludźmi, wystarczy chwila nieuwagi, pośpiech lub zmęczenie i nieszczęście gotowe. Jedno kliknięcie w złośliwy załącznik i wszystkie zdjęcie i dokumenty na dysku są zaszyfrowane.

„Dobrze sformułowana wiadomość e-mail wystarczy, aby zebrać dane logowania, uzyskać dostęp do poufnych informacji lub wstrzyknąć złośliwe oprogramowanie na docelowe komputery” – podkreślają autorzy podręcznika Cybersecurity All in One for Dummies (dodają, że **skuteczność phishingu sięga nawet 70 proc.** wysłanych wiadomości e-mail).

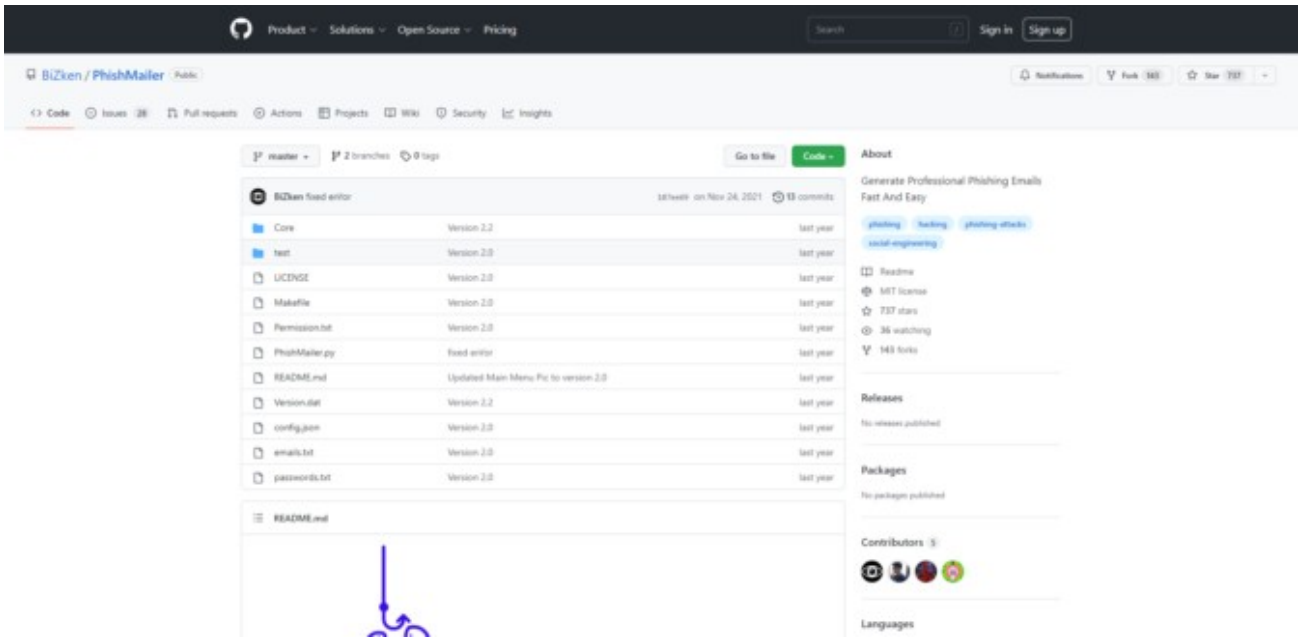
Spójrz, o czym należy pamiętać, aby maksymalnie poprawić bezpieczeństwo korzystania ze skrzynki pocztowej.

Jak bezpiecznie korzystać z poczty elektronicznej?

Każdy z nas dostał lub dostanie e-maila, który zawiera link do strony phishingowej lub załącznik z ukrytym ransomware lub trojanem.

To tylko kwestia czasu, bo przestępcy bardzo często **używają techniki „spray and pray”**. Zamiast wybierać ofiary stosują metodę, która kosztuje o wiele mniej pracy. Kupują w Darknecie dużą bazę z e-mailami i rozsyłają złośliwe wiadomości do setek tysięcy odbiorców. Im więcej wyślą e-maili, tym większa szansa, że ktoś popełni błąd i padnie ich ofiarą. Znajdziesz się na celowniku **nawet jeżeli nie jesteś prezesem wielkiej firmy lub bogatym człowiekiem**.

Oczywiście cyber łotry nadal próbują dostać się do skrzynki odbiorczej prezesów, urzędników i innych ważnych osób, żeby okraść ich z pieniędzy lub ważnych informacji (spear phishing).



Jak nie stać się łupem dla cyberprzestępców? Oto podstawowe zasady.

1. **Stosuj menedżer haseł** – wygenerujesz silne, unikalne hasła, których nie będziesz musiał zapamiętywać (program zrobi to za Ciebie). Dlaczego unikalne hasła są ważne? Przestępcy wiedzą, że większość osób używa tych samych haseł w różnych serwisach. Po przechwyceniu hasła sprawdzają czy pasuje one do innych usług (Facebooka, Gmail, Instagrama itd.).
2. **Korzystaj z jednorazowego adresu e mail** – nie zawsze musisz podawać swoje podstawowe adresy mailowe, do założenia konta na mniej ważnym/godnym zaufania serwisie użyj usługi np. Guerrilla Mail.
3. **Używaj pseudonimów e-mail (aliasów)**, czyli dodatkowych adresów Twojego konta pocztowego, które pomagają poprawić prywatność. Aliasy posłużą jako zastępcze adresy, kiedy nie chcesz używać swojego podstawowego adresu prywatnego lub firmowego – to alternatywa do zakładania nowej skrzynki lub użycia jednorazowego e-maila.
4. **Korzystaj z oprogramowania antywirusowego** na każdym urządzeniu, na którym odczytujesz wiadomości e-mail.
5. **Stosuj zasadę ograniczonego zaufania** przy podawaniu adresu e-mail – zdarzają się nieuczciwe sklepy online lub inne serwisy, które sprzedają dane swoich klientów. Używaj różnych adresów e-mail do różnych usług, odrębna skrzynka odbiorcza i nadawcza dla spraw służbowych, prywatnych i rozrywki to dobry pomysł.
6. **Nigdy nie otwieraj załączników w spamowych mailach** – to pewne źródło ransomware, trojanów i innych szkodników.
7. **Nie odpowiadaj na podejrzane maile** – przestępcy dostaną potwierdzenie, że Twój adres jest aktywny i mogą go również wykorzystać do socjotechnicznych ataków na innych użytkowników.
8. Przed kliknięciem w link lub załącznik **dokładnie przyjrzyj się wiadomości e-mail**, która trafiła do Twojej skrzynki pocztowej, sprawdź np. czy adres nadawcy jest poprawny (a nie zmienioną wersją zaufanej osoby/instytucji), czy wiadomość zawiera literówki, ma bardzo

ogólne zwroty grzecznościowe, trafiła do skrzynki odbiorczej w nocy, nakłania Cię do kliknięcia w linki/załącznik lub podanie poufnych danych, namawia do natychmiastowego działania.

9. Korzystaj ze sprawdzonej poczty elektronicznej **od zaufanego i dobrze znanego dostawcy**. To może być Gmail, poczta Yahoo, Proton Mail lub inna usługa, która odpowiada Twoim wymaganiom.
10. Jeżeli chcesz **sprawdzić odporność pracowników** firmy na phishingowe e-maile wykorzystaj platformy do generowanie testowych „złośliwych" wiadomości, LUCY (lucysecurity.com) lub Confese (cofense.com).

I na koniec: pamiętaj, aby nie ufać technologii bardziej niż człowiekowi. Dobra zasada, to **ograniczone zaufanie** – tak jak nie podasz swojego hasła do skrzynki pocztowej przypadkowej osobie spotkanej na ulicy, która twierdzi, że pracuje w Twoim banku, tak nie powinieneś wysyłać wrażliwych danych w odpowiedzi na e-mail twierdzący, że reprezentuje zaufaną instytucję.

Usługa poczty elektronicznej – pytania i odpowiedzi (Q&A)

Jaka poczta e-mail jest najlepsza?

Najlepsza poczta e-mail – z punktu widzenia zabezpieczeń – to Gmail od Google. Choć usługi cyfrowego giganta budzą kontrowersje ze względu na kwestie prywatności, to jest to z pewnością najbezpieczniejsza darmowa poczta elektroniczna.

Jaka alternatywa dla Gmail?

Jeżeli szukasz alternatywy dla Gmail, to rozważ konkurencyjne usługi poczty elektronicznej, np. Proton Mail z szyfrowaniem całej korespondencji po stronie klienta, Tutanota szyfrująca wszystkie dane z darmowym i anonimowym adresem e-mail, bezpłatny Outlook z 15 GB dla skrzynki odbiorczej i całego magazynu poczty, Yahoo Mail, który nie przypomina już poczty z początków internetu (ma przyjazny interfejs, wiele praktycznych funkcji i aż 1 TB pojemności) czy polską int.pl (należy do Interii), która nieźle chroni przed spamem, nie wysyła reklam, a jej skrzynka odbiorcza ma nieograniczoną pojemność (to nadal darmowa poczta). Osoby z dużą wiedzą techniczną mogą postawić własny serwer pocztowy.

Gdzie najlepiej założyć konto pocztowe?

Jeżeli zależy Ci na bezpieczeństwie wychodzących i przychodzących wiadomości, to wybierz Gmail. Osoby ceniące prywatność lub/i wysyłające dużo poufnych informacji mogą zdecydować się na pocztę elektroniczną z szyfrowaniem typu end-to-end (tylko nadawca i odbiorca mogą przeczytać wiadomość). Taką usługę znajdziesz np. w Proton Mail, Tutanota czy Mailvelope.