



ZAGROŻENIA BEZPIECZEŃSTWA QR NA FAKTURACH KSeF

Jak rozpoznać oszustów i chronić firmę?

Procedura zatwierdzenia faktur zmienia się z kodem QR na fakturach. QR to nie zatwierdzenie faktury – to fałszywe bezpieczeństwo, które oszuści z całą pewnością wykorzystają do phishingu. Gdy dostajesz mail z fakturą i QR-em, możesz trafić na fałszywą stronę lub otrzymać inną fakturę, niż oczekujesz. Poznaj trzy procedury weryfikacji (skanowanie, porównanie, weryfikacja KAS), które możesz dodać do instrukcji pracy. Prosta kontrola, która zatrzyma atak.

Spis treści

Zastrzeżenie.....	3
Praktyczny poradnik dla przedsiębiorców, księgowych i pracowników finansowych na 2026 r.	3
Czy to cię dotyczy?	3
TL;DR – Szybkie streszczenie jeśli się śpieszysz.....	3
Co to jest kod QR na fakturze KSeF i jak go bezpiecznie używać?.....	4
PRAKTYCZNY SCENARIUSZ: Jak oszuści wykorzystują QR do phishingu i kradzieży pieniędzy	4
Scenariusz 1: Fałszywa faktura mailem (najczęstszy atak)	4
Scenariusz 2: Zamieszana faktura.....	5
Główne zagrożenia – wyjaśnione prosto	5
Zagrożenie 1: Phishing – Jak oszust może wysłać Ci fałszywą stronę pod pozorem KSeF?	5
Zagrożenie 2: Zamieszana faktura – Dlaczego potwierdzona kwota może być inna niż faktyczna?	5
Zagrożenie 3: Ujawnienie informacji – Jak oszust pozoruje kolejną fakturę od Ciebie? .	6
Zagrożenie 4: Śledzenie – Co się dzieje, gdy QR prowadzi poza mf.gov.pl?	6
Zagrożenie 5: Złośliwe oprogramowanie – Czy zły QR może zaatakować mój telefon? .	7
JAK SIĘ BRONIĆ ? Konkretnie procedury dla wystawców i odbiorców faktur.....	7
Jeśli wystawiasz faktury (dla każdej firmy)	7
Jeśli odbierasz faktury (dla księgowych i pracowników finansowych)	7
PROCEDURA 1: Bezpieczne skanowanie QR.....	7
PROCEDURA 2: Jak weryfikować rachunek bankowy dostawcy bez ryzyka? (Accounts Payable).....	8
PROCEDURA 3: Zatwierdź i zapłać (ostateczna obrona)	8
NAJWAŻNIEJSZE ZASADY – szybka ściągawka.....	9
PYTANIA I ODPOWIEDZI	9
Podsumowanie	10
Jak użyć tego artykułu z AI?.....	10
Oświadczenie	11
Kolejne kroki	11

Zastrzeżenie

Niniejszy materiał ma charakter wyłącznie informacyjny i edukacyjny. Nie stanowi porady prawnej, podatkowej ani księgowej i nie może być traktowany jako oficjalna wykładnia prawa. Każdy podatnik powinien samodzielnie ocenić swoją sytuację lub skonsultować się z doradcą, a także na bieżąco śledzić zmiany przepisów, objaśnienia Ministerstwa Finansów oraz orzecznictwo sądów i interpretacje organów podatkowych.

Autorzy nie ponoszą odpowiedzialności za skutki decyzji podjętych wyłącznie na podstawie tego opracowania; w razie wątpliwości konieczna jest indywidualna analiza przepisów mających zastosowanie w danym stanie faktycznym.

Praktyczny poradnik dla przedsiębiorców, księgowych i pracowników finansowych na 2026 r.

Od 1 lutego 2026 r. każda faktura wysłana mailem lub w formie PDF musi zawierać kod QR prowadzący do systemu KSeF. To narzędzie ma zwiększać bezpieczeństwo i ułatwiać weryfikację dokumentów – ale oszuści już nauczyli się je wykorzystywać. Ten artykuł pokazuje konkretne zagrożenia oraz proste procedury, które możesz wdrożyć w firmie, aby skutecznie się bronić.

Czy to cię dotyczy?

TAK, jeśli:

- Wysyłasz faktury (mailem, PDF, wydruk) – musisz upewnić się, że QR na Twojej fakturze jest bezpieczny
- Odbierasz faktury od dostawców – musisz wiedzieć, jak bezpiecznie zeskanować QR i nie dać się oszukać

Czytaj artykuł, aby dowiedzieć się, jak oszuści mogą Cię oszukać przez QR i co konkretnie robić, aby się bronić.

TL;DR – Szybkie streszczenie jeśli się śpieszysz

Jeśli nie masz czasu czytać cały artykuł, zapamiętaj TO:

- **Jeśli nie musisz, nie korzystaj z wizualizacji faktury przestanej do KSeF! API jest pewnym źródłem informacji, wizualizacja NIE!**
- **QR ≠ gwarancja** – to tylko potwierdzenie, że faktura istnieje w KSeF
- **Zawsze sprawdzaj domenę:** podatki.gov.pl (nic innego)
- **Rachunek z kartoteki:** nie z PDF-a; weryfikuj na liście KAS
- **Wątpisz?** – dzwoń do dostawcy telefonicznie
- **Procedury:** wystarczą 3 minuty na fakturę, aby uniknąć strat tysięcy złotych

Wdróż to w swoim zespole dziś – podziękujesz sobie za miesiąc.

Co to jest kod QR na fakturze KSeF i jak go bezpiecznie używać?

Od 1 lutego 2026 r., faktury wysyłane mailem lub w formie PDF muszą zawierać kod QR. Kiedy go zeskanujesz telefonem, trafiasz na stronę rządową (mf.gov.pl), gdzie możesz sprawdzić, czy faktura rzeczywiście istnieje w systemie KSeF.

Jak to działa w praktyce:

1. Zeskanujesz QR na fakturze telefonem
2. Widzisz podstawowe dane: NIP sprzedawcy, numer faktury, kwota
3. System pyta: „Czy chcesz pobrać całą fakturę?”
4. Aby pobrać, musisz wpisać: numer faktury i kwotę (dane, które i tak są na dokumencie)

Kluczowa informacja: Kod QR zawiera tylko informacje, które są już widoczne na samej fakturze. Nic poufnego.

Czego nie widzisz ani w kodzie QR, ani na stronie MF?

1. Nie widzisz kwoty faktury
2. Nie widzisz konta bankowego

To jest miejsce potencjalnego ataku. Faktura sfalszowana może mieć zawyżoną kwotę i konto bankowe oszustów! Tego nie zweryfikujesz korzystając z kodu QR.

PRAKTYCZNY SCENARIUSZ:

Jak oszuści wykorzystują QR do phishingu i kradzieży pieniędzy

Zanim wyjaśnię zagrożenia abstrakcyjnie, oto konkretny przykład, który pokazuje, jak to wygląda w rzeczywistości:

Scenariusz 1: Fałszywa faktura mailem (najczęstszy atak)

1. Dostajesz wiadomość mailową:

„Oto Twoja faktura do zapłaty nr 2026/001 od firmy ABC Sp. z o.o. – Należność: 10 000 zł. Proszę przelać przelew na konto: 12345678...”

W mailu jest załącznik PDF z kodem QR.

2. Zeskanujesz QR telefonem.

Trafiasz na stronę wyglądającą dokładnie jak podatki.gov.pl (ale to strona oszusta). Widzisz napis: „Faktura znaleziona w KSeF ✓”.

3. Klikasz „Pobierz” i pojawia się wiadomość:

„Aby pobrać fakturę, przepraszamy, ale najpierw musisz opłacić prowizję: 1 zł. Prześlij przelew na konto...”

4. **Co robisz?** Wysyłasz ten 1 zł, myśląc, że to procedura weryfikacyjna.
5. **Efekt:** Twoje pieniądze idą na konto oszusta. Nigdy nie otrzymujesz faktury. Cała procedura wyglądała wiarygodnie, bo QR rzeczywiście prowadził do „weryfikacji”.

Scenariusz 2: Zamieszana faktura

1. Dostajesz fakturę od znanego dostawcy (np. o kwotę 500 zł).
2. Zeskanujesz QR – „Faktura w KSeF ✓”.
3. Ale w rzeczywistości oszust wysłał inną fakturę, na inną kwotę (np. 5 000 zł) od tego samego dostawcy.
4. Ty widzisz tylko „weryfikacja przeszła” i płacisz 5 000 zł zamiast 500 zł.

Główne zagrożenia – wyjaśnione prosto

Zagrożenie 1: Phishing – Jak oszust może wysłać Ci fałszywą stronę pod pozorem KSeF?

Co się dzieje: Oszust posyła Ci wiadomość mailową z PDF-em i QR-em, ale QR prowadzi nie na podatki.gov.pl, tylko na podrobioną stronę. Kiedy zeskanujesz, trafiasz na stronę wyglądającą identycznie jak rządowa, ale obsługiwana przez oszusta.

Dlaczego to działa:

- QR to „klik bez czytania” – nie czytasz adresu, który się otwiera
- Oszust może postać Ci stronę wyglądającą 100% identycznie, z tym samym logo, takim samym kolorami
- Nawet doświadczeni użytkownicy mogą nie zauważyć różnicy

Jak się chronić:

1. **Zeskanuj QR, ale NIE KLIKAJ od razu** – zamiast tego użyj aplikacji, która pokazuje adres **przed** otwarciem linku
2. **Ręcznie sprawdź adres:** Prawidłowy adres to podatki.gov.pl – nic więcej, nic mniej
3. **Uważaj na literówki:** Oszust może użyć podobnie wyglądających znaków – w pośpiechu nie zauważysz

Zagrożenie 2: Zamieszana faktura – Dlaczego potwierdzona kwota może być inna niż faktyczna?

Co się dzieje: Nawet jeśli QR potwierdzi, że faktura istnieje w KSeF, oszust może wysłać Ci **inną** fakturę od tego samego dostawcy.

Przykład:

- Zamawiasz na 500 zł i dostajesz fakturę od firmy ABC
- Oszust wysyła Ci inną fakturę od ABC, ale za 5 000 zł
- Zeskanujesz QR – „Faktura w KSeF ✓”

- Płacisz 5 000 zł zamiast 500 zł

Dlaczego to się dzieje: QR potwierdza tylko, że **jakaś** faktura od tej firmy istnieje w KSeF. Nie potwierdza, że to jest **ta konkretna** faktura, którą Ty oczekujesz.

Jak się chronić:

1. **Zawsze porównaj dane z fakturą z Twoją kartoteką dostawcy:**
 - NIP dostawcy – czy zgadza się?
 - Numer faktury – czy to liczba, którą oczekujesz?
 - Kwota – czy to jest poprawna kwota?
 - Rachunek bankowy – czy to konto, na które zawsze płacisz?
2. **Jeśli cokolwiek nie zgadza się** – skontaktuj się z dostawcą telefonicznie ZANIM zapłacisz
3. **Nigdy nie ufaj rachunkowi bankowemu z PDF-a** – zawsze sprawdź w swojej kartotece i na oficjalnej liście kont bankowych KAS (<https://podatki-arch.mf.gov.pl/wykaz-podatnikow-vat-wyszukiwarka/>)

Zagrożenie 3: Ujawnienie informacji – Jak oszust pozoruje kolejną fakturę od Ciebie?

Co się dzieje: Jeśli ktoś dostanie PDF-a z Twoją fakturą (np. przez przypadkowy forward maila, wydruk, screenshot), będzie znać Twój NIP, datę wystawienia i numer faktury. Może to wykorzystać, aby pozorować kolejną fakturę od Ciebie.

Przykład:

- Oszust widzi, że wystawiłeś fakturę 15.01.2026
- Wysła wiadomość do Twojego klienta: „Oto korekta faktury z 15.01.2026. Prosimy o dodatkowe 2000 zł...”
- Twój klient myśli, że to wiadomość od Ciebie

Jak się chronić:

- Wysyłaj faktury kanałami bezpiecznym (szyfrowana poczta, portal B2B, EDI)
- Jeśli wysyłasz mailem, upewnij się, że wiadomość jest szyfrowana
- Edukuj swoich pracowników: upewnij się, że znają Twój główny numer telefonu, aby mogą weryfikować dziwne próśby

Zagrożenie 4: Śledzenie – Co się dzieje, gdy QR prowadzi poza mf.gov.pl?

Co się dzieje: Jeśli QR prowadzi gdziekolwiek poza mf.gov.pl, Twój telefon może być śledzony – czyli kto, kiedy i z jakiego miejsca skanował QR.

Dlaczego to ma znaczenie: To nie jest „wyciek danych osobowych“, ale może być używane do celów analitycznych lub mogą być zbierane informacje o Twoim teamie/działach.

Jak się chronić:

- **Zawsze skanuj QR prowadzący do mf.gov.pl** – to strona rządowa

- Jeśli QR prowadzi gdziekolwiek indziej – skonsultuj się z zespołem IT zanim skanujesz

Zagrożenie 5: Złośliwe oprogramowanie – Czy zły QR może zaatakować mój telefon?

Co się dzieje: Złośliwa strona (do której prowadzi QR) może próbować zaatakować Twoją przeglądarkę mobilną i zainstalować złośliwe oprogramowanie.

Jak się chronić:

- Zawsze skanuj QR aplikacją, która pokazuje adres linku **przed** kliknięciem
- Nie klikaj w linki z nieznanych źródeł
- Miej aktualny system operacyjny na telefonie

JAK SIĘ BRONIĆ ?

Konkretne procedury dla wystawców i odbiorców faktur

Jeśli wystawiasz faktury (dla każdej firmy)

1. **Upewnij się, że QR na Twojej fakturze prowadzi do subdomeny mf.gov.pl**
 - Skontaktuj się z Twoim dostawcą ERP-u lub systemu fakturowania
 - Poproś, aby sprawdzili, czy konfiguracja QR jest prawidłowa

2. **Pod kodem QR drukuj czytelnie:**

xxx.mf.gov.pl

Dzięki temu, jeśli ktoś zmodyfikuje QR, odbiorcy mogą to łatwo sprawdzić, porównując domenę na wydruku z adresem, na który trafia po zeskanowaniu.

1. **Wysyłaj faktury bezpiecznie**
 - Jeśli to możliwe, wysyłaj przez portal B2B (zamiast maila)
 - Jeśli wysyłasz mailem, używaj szyfrowania
 - Papierowe kopie przechowuj w zamkniętym magazynie
2. **Podpisz PDF-a cyfrowo** (jeśli Twój system to umożliwia)
 - Jeśli ktoś zmieni QR na PDF-ie, podpis cyfrowy to wykaże
 - Odbiorcy mogą to sprawdzić przed zapłatą
3. **Edukuj swój zespół**
 - Wyjaśnij pracownikom, że wysyłanie kopii faktury mailem powinno być wyjątkiem, nie regułą
 - Jeśli ktoś wysyła faktury, upewnij się, że wie o zagrożeniach phishingiem

Jeśli odbierasz faktury (dla księgowych i pracowników finansowych)

PROCEDURA 1: Bezpieczne skanowanie QR

1. **Przeszkolenie pracowników:**
 - Kiedy odbierasz mail z fakturą i QR-em, STOP – nie skanuj od razu
 - Najpierw sprawdź, czy mail pochodzi od znanego kontrahenta (sprawdź adres mailowy)

- Teraz zeskanuj QR aplikacją, która pokazuje adres PRZED kliknięciem
 - Rekomendujemy: aplikacja KSeF (od 1 lutego 2026) lub scanner wskazujący URL
- 2. **Sprawdzenie domeny:**
 - Czy adres to podatki.gov.pl? DOBRZE
 - Czy adres to coś innego? – skontaktuj się z IT, zanim pójdziesz dalej
- 3. **Po zeskanowaniu:**
 - Zapisz sobie dane: NIP dostawcy, numer faktury, kwota
 - Przejdź do następnego kroku (patrz: PROCEDURA 2)

PROCEDURA 2: Jak weryfikować rachunek bankowy dostawcy bez ryzyka?
(Accounts Payable)

NIGDY nie zatwierdzaj faktury na podstawie samego QR!

4. **Porównaj dane z fakturą z Twoją kartoteką dostawcy:**
 - [] NIP dostawcy – czy zgadza się z kartoteką?
 - [] Numer faktury – czy to poprawny numer?
 - [] Kwota brutto – czy to jest kwota, którą oczekujesz?
 - [] Data wystawienia – czy to logiczna data (np. nie z przyszłości)?
 - [] Rachunek bankowy – czy to jest konto, na które zawsze płacisz?
(sprawdź w ERP-ie, NIE na PDF-ie!)
5. **Weryfikacja rachunku bankowego dostawcy:**
 - Zawsze sprawdź rachunek w **Wykazie podatników VAT prowadzonym przez KAS** – to oficjalna lista zweryfikowanych kont bankowych
 - Link do weryfikacji: <https://podatki-arch.mf.gov.pl/wykaz-podatnikow-vat-wyszukiwarka/>
 - Wpisz NIP dostawcy i sprawdź, czy rachunek z faktury jest na liście
 - **Jeśli rachunek nie jest na liście KAS – STOP, nie płacić, skontaktować się z dostawcą telefonicznie**
6. **Jeśli cokolwiek nie zgadza się:**
 - STOP – nie płacić
 - Skontaktuj się z dostawcą **telefonicznie** (nie mailem!) i potwierdź: „Czy wystawiłeś mi fakturę nr 2026/001 na kwotę 10 000 zł?”
 - Dopiero jeśli potwierdzi – zatwierdź fakturę w systemie
7. **Zwróć szczególną uwagę na:**
 - Zmianę rachunku bankowego
 - Zmianę NIP-u dostawcy
 - Kwoty znacznie wyższe niż zwykle
 - Faktury od nowych dostawców (aplikuj bardziej surowe sprawdzenie)

PROCEDURA 3: Zatwierdź i zapłać (ostateczna obrona)

1. **Zatwierdź fakturę w ERP-ie** (po przejściu procedury 1 i 2)
2. **Przygotuj przelew**, ale zanim klikniesz „wyślij“:

- [] Rachunek bankowy w przelewie – sprawdzony z kartoteką w ERP-ie i zweryfikowany na liście KAS?
 - [] Kwota zgadza się z fakturą?
 - [] Wszystkie dane kontrahenta zgadzają się?
3. **Wyślij przelew**
 4. **Zapisz potwierdzenie** (nr referencji banku, data, godzina)

NAJWAŻNIEJSZE ZASADY – szybka ściągawka

Zapamiętaj te 5 reguł, aby nie być oszukanym:

1. **QR NIE zatwierdza faktury** – to tylko dodatkowy sygnał, że dokument istnieje w systemie. Zawsze porównaj z kartoteką dostawcy.
2. **Zawsze sprawdź NIP dostawcy** – jeśli na fakturze jest inny niż w Twojej kartotece, STOP – skontaktuj się z dostawcą.
3. **Rachunek bankowy biorą z kartoteki i weryfikują na liście KAS, NIE z PDF-a** – jeśli PDF zawiera inny rachunek, to czerwona flaga.
4. **Jeśli QR prowadzi poza podatki.gov.pl** – pytaj się IT zanim skanujesz. Prawdziwe QR-y prowadzą tylko na stronę rządową.
5. **Wątpisz?** – zawsze zadzwoń do dostawcy i potwierdź telefonicznie. To zajmie 2 minuty i zabezpieczy Ciebie przed stratą tysięcy złotych.

PYTANIA I ODPOWIEDZI

P: Czy mogę skanować QR z każdego telefonu?

O: Tak, ale lepiej użyj aplikacji, która pokazuje adres linku przed otwarciem (np. aplikacja KSeF od 1 lutego 2026). Zwykły skaner QR też działa, ale musisz być bardziej ostrożny.

P: Co jeśli QR nie działa?

O: To może oznaczać, że: (1) strona jest niedostępna, (2) QR jest uszkodzony, (3) QR prowadzi na błędny adres. Skontaktuj się z dostawcą/IT, aby sprawdzili.

P: Czy mogę wysyłać faktury mailem?

O: Tak, ale upewnij się, że:

- Mail jest od znanego kontrahenta (sprawdź adres mailowy)
- PDF zawiera QR prowadzący na podatki.gov.pl
- Wysyłaj szyfrowaną pocztą (jeśli Twoja firma to umożliwia)

P: Co jeśli jestem małym przedsiębiorcą i nie mam ERP-u?

O: To samo – zawsze porównaj dane z faktury z Twoją kartoteką dostawcy (nawet jeśli trzymasz ją w Excelu). Nigdy nie płać na rachunek z PDF-a bez wcześniejszej weryfikacji.

P: Czy QR zawiera moje dane osobowe? O: Nie. QR zawiera tylko informacje widoczne na fakturze: datę, NIP dostawcy, numer. Nic poufnego.

P: Gdzie sprawdzić, czy rachunek bankowy dostawcy jest prawidłowy? O: W Wykazie podatników VAT prowadzonym przez KAS: <https://podatki-arch.mf.gov.pl/wykaz-podatnikow-vat-wyszukiwarka/> Wpisz NIP dostawcy, a system pokaże wszystkie rachunki bankowe powiązane z tą firmą.

Podsumowanie

Kod QR na fakturze KSeF to narzędzie mające ułatwić Ci życie – pozwala szybko sprawdzić, czy faktura istnieje w systemie rządowym. Jednak **QR sam w sobie NIE gwarantuje, że faktura jest prawidłowa.**

Najczęstsze zagrożenia to:

1. **Phishing** – oszust posyła Ci QR prowadzący na fałszywą stronę
2. **Zamieszana faktura** – QR potwierdza, że faktura istnieje, ale to nie ta faktura, którą oczekujesz
3. **Ujawnienie danych** – jeśli ktoś dostanie Twoją fakturę, może pozorować kolejną

Aby się chronić, wystarczy:

- Sprawdzić domenę w adresie linku (musi być podatki.gov.pl)
- Porównać dane z faktury z kartoteką dostawcy
- Zweryfikować rachunek bankowy na liście KAS
- Nigdy nie ufać rachunkowi bankowemu z PDF-a
- Zadzwoń do dostawcy, jeśli coś nie zgadza się

To proste, ale efektywne. Wdrożenie tych procedur zajmie Tobie kilka minut dziennie, ale zabezpieczy Twoją firmę przed stratą tysięcy złotych.

Jak użyć tego artykułu z AI?

Jeśli używasz asystenta AI do:

- **Tworzenia procedur** wewnętrznych: Skopiuj sekcję „JAK SIĘ BRONIĆ” i dostosuj do swojego systemu ERP
- **Szkolenia zespołu:** Użyj scenariuszy praktycznych (Scenariusz 1 i 2) jako studium przypadku
- **Audytu:** Przejrzyj procedury 1–3 razem z działem IT i działem finansowym
- **Automatyzacji:** Procedura 2 (weryfikacja dostawcy i rachunku) może być częściowo zautomatyzowana w procesach AP

Tekst artykułu zawiera gotowe do wdrożenia procedury – nie musisz nic wymyślać od nowa.

Oświadczenie

Artykuł został napisany na podstawie oficjalnych źródeł Ministerstwa Finansów dotyczących systemu KSeF i zawiera praktyczne rekomendacje bezpieczeństwa dla przedsiębiorców i księgowych.

Kolejne kroki

Wdrożyć powyższe procedury w Twojej firmie:

1. Sprawdzić konfigurację QR w systemie ERP-u
2. Przeszkolić zespół finansowy na temat procedury weryfikacji
3. Zaktualizować procedury AP (Accounts Payable) w firmie
4. Udostępnić artykuł pracownikom zajmującym się fakturami

Dokument przygotowany: styczeń 2026

Dla: Przedsiębiorcy, księgowi, pracownicy finansowi

Wersja: 1.0

Licencja: Materiał edukacyjny do swobodnego użytku (z podaniem źródła)