

**PIERWSZE URUCHOMIENIE**

Cztery komunikaty, zero zaskoczenia.

Instrukcja dla obecnej wersji HC Tender Control: Windows, macOS, Android Play Protect i pierwsze logowanie Google. Wszystkie ekrany dotyczą wyłącznie pierwszego uruchomienia, instalacji albo pierwszej autoryzacji.

DLACZEGO POJAWIAJĄ SIĘ KOMUNIKATY

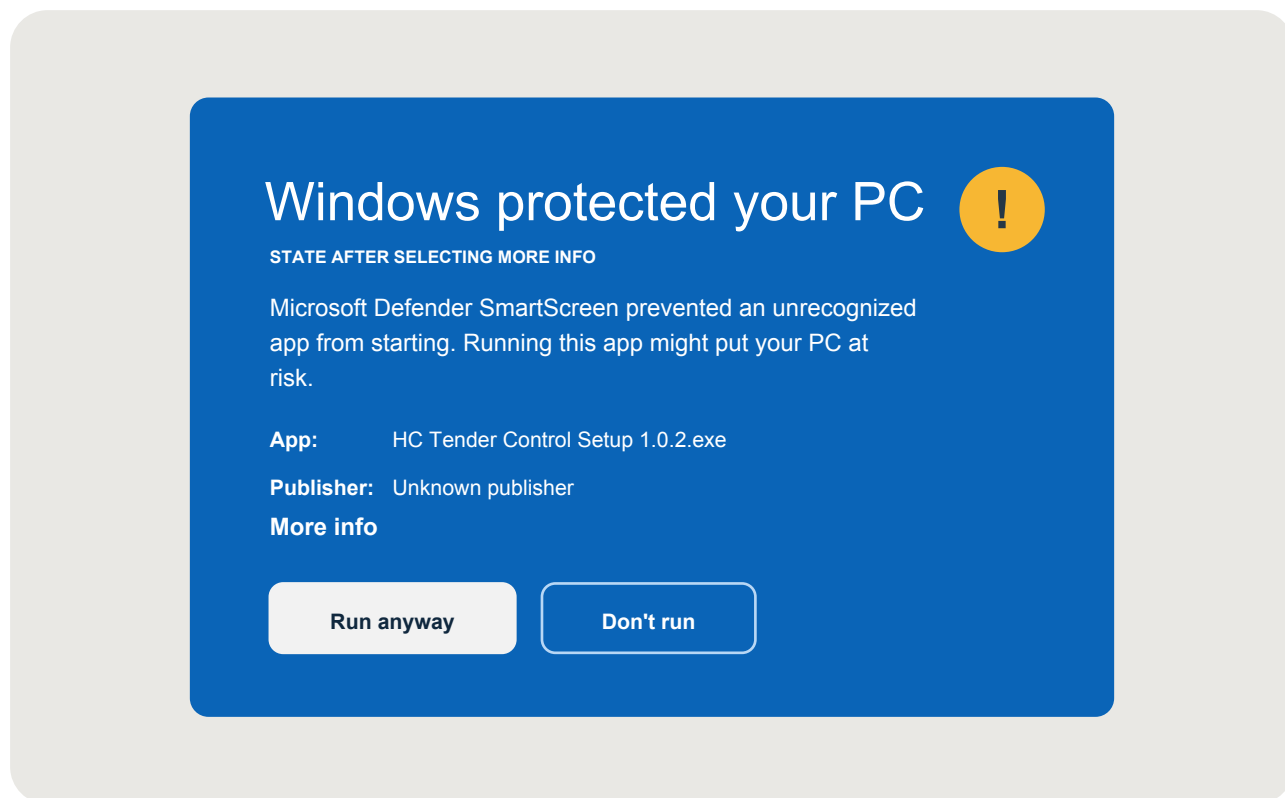
Instalatory nie są jeszcze podpisane certyfikatem wydawcy rozpoznawanym przez Windows ani podpisane i notaryzowane przez Apple. Android może zaproponować skan Play Protect, a Google OAuth oczekuje na weryfikację. Firma otrzymuje tę informację przed pilotażem, a instalację przechodzimy wspólnie.

Nie wyłączaj SmartScreen, Gatekeeper, Play Protect ani ochrony konta Google. Kontynuuj tylko z plikiem otrzymanym bezpośrednio od Hazards Control. W firmowym środowisku zarządzanym decyzję może podjąć wyłącznie administrator IT.

01 / WINDOWS 10 I 11

Jak przejść ekran SmartScreen

Po uruchomieniu pliku HC Tender Control Setup 1.0.2.exe SmartScreen może pokazać poniższy ekran. Kliknij More info / Więcej informacji, sprawdź nazwę pliku i wybierz Run anyway / Uruchom mimo to. Nie wybieraj tej opcji dla pliku z innego źródła.

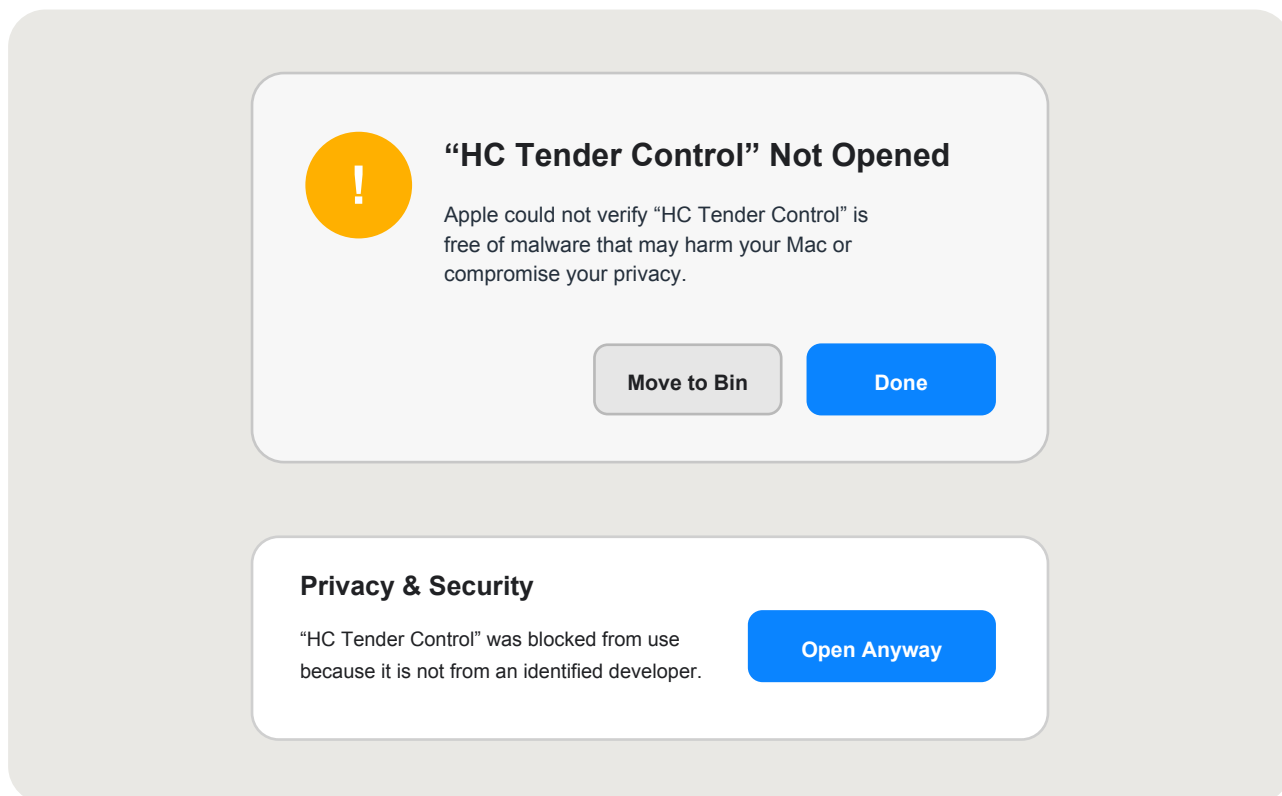


Rekonstrukcja standardowego ekranu SmartScreen. Kolor i układ mogą nieznacznie różnić się zależnie od wersji Windows i polityki firmy.

02 / macOS

Jak otworzyć aplikację na macOS

- Spróbuj otworzyć HC Tender Control i zamknij pierwszy komunikat przyciskiem Gotowe / Done.
- Otwórz Ustawienia systemowe → Prywatność i ochrona, przewiń do sekcji Ochrona i kliknij Otwórz mimo to / Open Anyway.
- Potwierdź hasłem lub Touch ID, a w ponownym komunikacie wybierz Otwórz / Open.

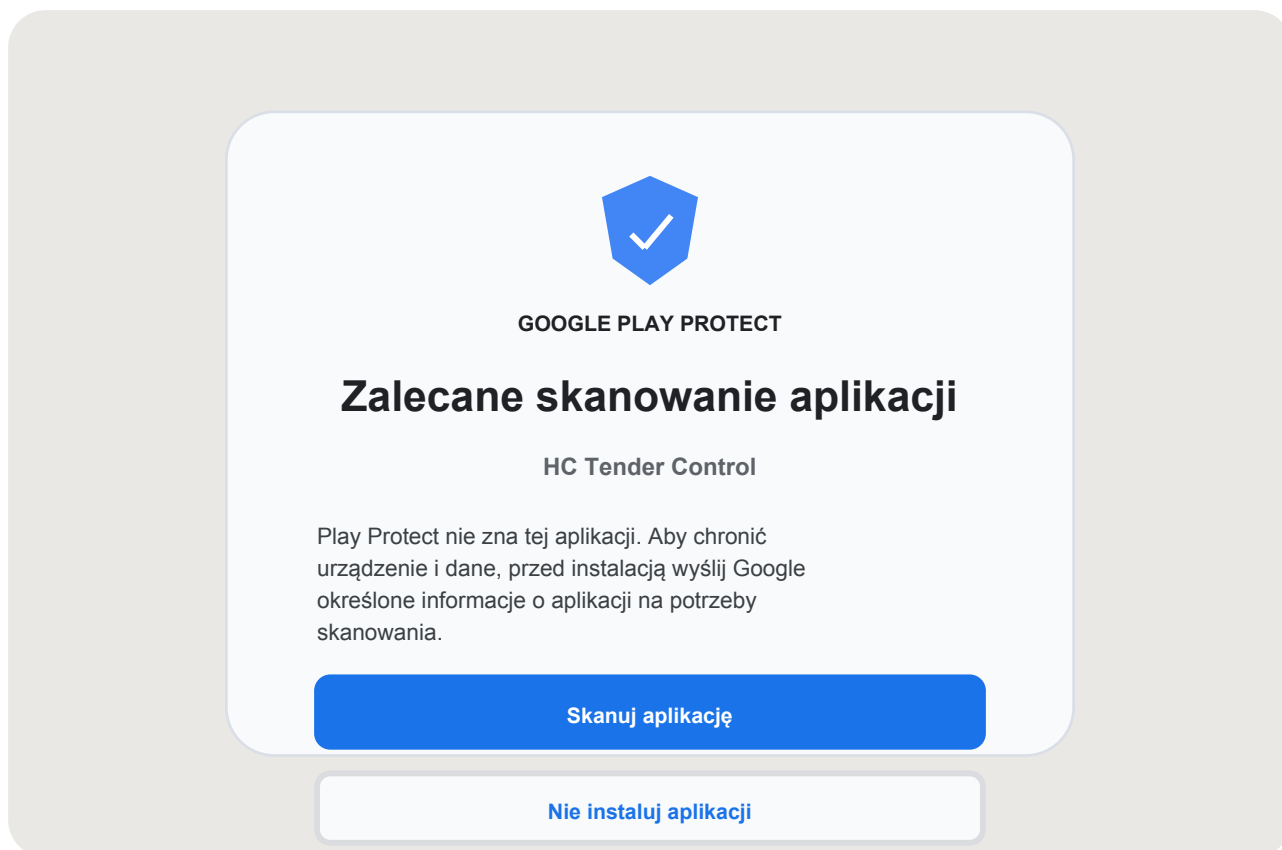


Przycisk Open Anyway jest według Apple dostępny przez około godzinę od pierwszej próby otwarcia. Na komputerze zarządzanym może go nie być.

03 / ANDROID I PLAY PROTECT

Najpierw skan, potem instalacja

Podczas instalowania pliku APK spoza Google Play system może wyświetlić komunikat „Zalecane skanowanie aplikacji”. Zalecana ścieżka to „Skanuj aplikację” i oczekiwanie na wynik Play Protect. Po komunikacie, że aplikacja wygląda na bezpieczną, kontynuuj instalację.

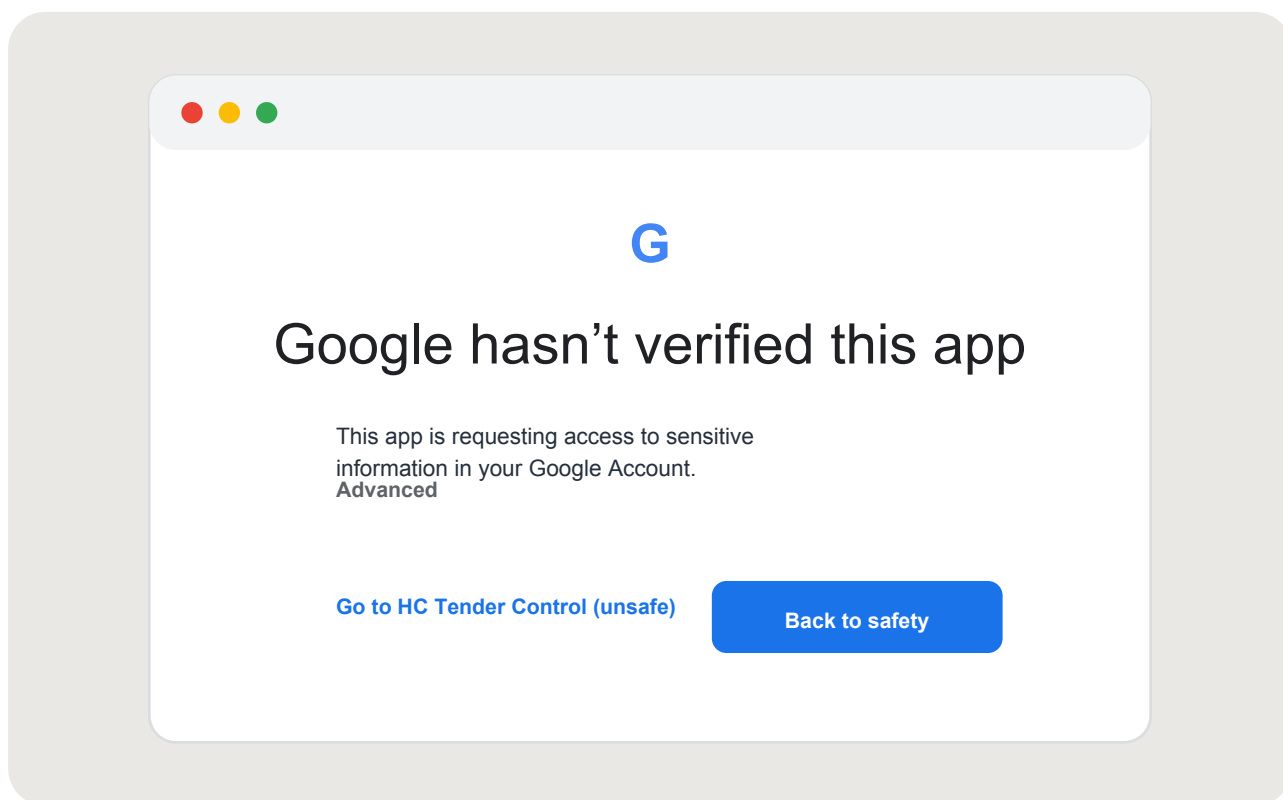


Na części urządzeń po rozwinięciu Więcej informacji / More details może pojawić się opcja Zainstaluj mimo to / Install anyway albo Install without scanning. Nie jest to jednolity element Androida i może go nie być. Instrukcja nie zaleca wyłączania Play Protect; jeżeli skan lub instalacja są blokowane przez politykę firmy, skontaktuj się z administratorem IT.

04 / PIERWSZE LOGOWANIE GOOGLE

Zaawansowane → przejdź do HC Tender Control

Google może wyświetlić ekran „Google nie zweryfikował tej aplikacji”. Wybierz Zaawansowane / Advanced, następnie Otwórz HC Tender Control / Go to HC Tender Control i przeczytaj zakresy na właściwym ekranie zgody. Zatwierdź tylko konto przeznaczone do wdrożenia.



Jeżeli widzisz Error 403: access_denied albo nie ma linku kontynuacji, nie próbuj obchodzić blokady. Konto musi zostać dopuszczone do projektu albo zatwierdzone przez administratora Google Workspace.

POTWIERDZENIE I WSPARCIE

Co sprawdzić przed kliknięciem

- Plik ma nazwę HC Tender Control Setup 1.0.2.exe na Windows albo HC Tender Control-1.0.2-arm64.dmg na komputerze Mac z Apple Silicon.
- Na Androidzie nazwa i wersja pliku APK są zgodne z informacją przekazaną przez Hazards Control.
- Plik został przekazany bezpośrednio przez Hazards Control w ustalonym kanale.
- Konto Google jest tym, które zostało ustalone dla wdrożenia.
- Na komputerze firmowym administrator IT zgodził się na instalację.

POMOC PRZY INSTALACJI

Instalacja i pierwsze logowanie są wykonywane wspólnie podczas umówionego wdrożenia. Kontakt: sforowicz@hazardscontrol.pl.

Źródła producentów zabezpieczeń

Apple Support: support.apple.com/guide/mac-help/open-a-mac-app-from-an-unknown-developer-mh40616/mac

Microsoft Learn: learn.microsoft.com/windows/apps/package-and-deploy/smartscreen-reputation

Google Cloud Help: support.google.com/googleapi/answer/7454865

Google Play Protect: developers.google.com/android/play-protect/warning-dev-guidance

Dokument odwzorowuje standardowe komunikaty i właściwą kolejność działań dla obecnej wersji produktu. Tekst i układ systemowych okien mogą różnić się językiem, wersją systemu albo polityką administratora.