MFA, passkeys i niezamówione kody logowania

Drugi etap logowania utrudnia przej?cie konta, ale nie ka?de potwierdzenie nale?y zatwierdza?.

LCPD / DATPOL · aktualizacja: 24.10.2026 · materia? do dopasowania do procedur organizacji.

Wybór metody

Preferuj zatwierdzone passkeys lub klucze FIDO2 odporne na phishing. Gdy nie s? dost?pne, u?yj aplikacji uwierzytelniaj?cej; SMS mo?e by? rozwi?zaniem przej?ciowym. Dwa has?a to nie dwa niezale?ne czynniki. Kodu nie podawaj osobie przedstawiaj?cej si? jako informatyk.

Nieoczekiwane powiadomienie

Nie zatwierdzaj. Zapisz czas i us?ug?, zg?o? do IT. Seria powiadomie? mo?e mie? zm?czy? u?ytkownika. Zgodno?? numeru na ekranie tak?e nie uprawnia do akceptacji, je?li nie rozpocz??e? logowania.

Utrata telefonu

Zg?o? natychmiast. IT odwo?uje stare uwierzytelniacze i sesje oraz potwierdza to?samo?? ustalonym kana?em. Przy planowanej wymianie najpierw dodaj i przetestuj now? metod?. Nie twórz wspólnego telefonu uwierzytelniaj ?cego wszystkich administratorów.

Sprawdź w praktyce

- Akceptuj? wy??cznie w?asne logowania.
- Nie pokazuj? kodu ani ekranu z kodem.
- Mam bezpieczn? metod? odzyskania.

Sytuacja z pracy

„Prosz? zaakceptowa? powiadomienie, testujemy system”. Odmawiasz i sam dzwonisz na znany numer IT.

Źródła i dalsza lektura

- NIST SP 800-63B-4
- ENISA — cyberhigiena

BHP w IT na LCPD: zasady i szybkie dzia?ania

W podręczniku BHP w IT

Wszystkie tematy i rozdzia?y

Poprzedni temat: Has?a, mened?er hase? i bezpieczna zmiana

Nast?pny temat: Pendrive, dysk USB i obce akcesoria

Wersja #2
Utworzono 2026-10-24 07:56:51 UTC przez Administrator DATPOL
Zaktualizowano 2026-10-24 07:56:52 UTC przez Administrator DATPOL