MUNI
FAKULTA
SOCIÁLNÍCH
STUDIÍ

MUNI
FAKULTA
INFORMATIKY

Uživatelské testování autentizačních metod mobilního bankovnictví

UX testování, rozhovory s uživateli a kvantitativní šetření

Technická zpráva projektu TA ČR *Inovace a adaptace autentizačních technologií pro bezpečné digitální prostředí (TL01000207)*

Autoři:

Mgr. Agáta Kružíková

Mgr. Lenka Knapová

Mgr. Ondřej Gabrhelík

Prof. PhDr. David Šmahel, Ph.D.

Mgr. Lenka Dědková, Ph.D.

Prof. RNDr. Václav Matyáš, M.Sc., Ph.D.

Mgr. Petr Doležal

Mgr. Martina Šmahelová, Ph.D.

MUNI Interdisciplinary Research Team on Internet and Society

CROCS

KLÍČOVÁ ZJIŠTĚNÍ

Tato zpráva popisuje výstupy testování autentizačních metod a aplikací pro chytré telefony spolu s metodikou použitou pro toto testování. Snažíme se zodpovědět otázku, které autentizační metody jsou koncovými uživateli vnímány jako bezpečné a uživatelsky přívětivé a které metody by uživatelé preferovali, pokud by měli možnost volby. Tato technická zpráva může být zajímavá pro bezpečnostní experty, manažery bezpečnosti IT, odborníky na UX a výzkumníky v oblasti použitelné bezpečnosti. Zpráva jim může pomoci pochopit hodnocení uživatelů a faktory, které jej ovlivňují.

Dokument má tři části: (1) Bezpečnost a hrozby vybraných autentizačních metod: technická specifikace, (2) UX testování a rozhovory s uživateli (3) Kvantitativní šetření dospělé a stárnoucí populace. Následuje shrnutí klíčových bodů těchto tří částí, v textu najdete odkazy na detailnější informace, které jsou dále v technické zprávě.

(1) Klíčová fakta: Bezpečnost a hrozby vybraných autentizačních metod: technická specifikace

Následující autentizační metody byly implementovány pro použití na chytrých telefonech (s OS Android): SMS kód, PIN, otisk prstu, FIDO token, identifikační karta s čipem (platební karta) přiložená ke čtečce NFC nebo vložená do čtečky karet a NFC token. Silné a slabé stránky zmíněných metod jsou detailně popsány zde. Technickou specifikaci metod lze shrnout následovně:

- Jednorázový SMS kód: Jedna z nejčastěji používaných metod v rámci dvoufaktorové autentizace. Jeho výhodou je jednoduchá implementace, nevýhodou pak cena za každou SMS a časté útoky, kdy je SMS přesměrována útočníkovi.
- PIN kód: Často používaná metoda, která je ovšem z hlediska bezpečnosti pro některé finanční operace nedostatečná díky mnohdy jednoduše proveditelným útokům, jako je odpozorování, sociální inženýrství, odhadnutí, použití keyloggeru, překrytí či odposlechnutí.
- Otisk prstu: Slibná metoda díky své uživatelské přívětivosti, která ale nezajišťuje příliš vysokou bezpečnost kvůli nedostatečně kvalitní implementaci na mobilních telefonech (např. absence kontroly živosti) a existenci masterprint útoků.
- FIDO token: Metoda založena na silné asymetrické kryptografii podléhající certifikaci. Z principu (uložení libovolných kryptografických klíčů na libovolný FIDO token) nemůže mít banka žádnou kontrolu nad tím, kdo token vlastní a k jakým dalším službám jej používá.
- Identifikační karta s čipem (platební karta): Zatím vzácně používaná metoda, a to jak v případě načtení přes NFC čtečku chytrého telefonu, tak při vložení do čtečky karet. Bezpečnost záleží vždy na konkrétní implementaci kryptografických algoritmů, funkcí a klíčů, ale obecně jsou čipové karty nejsilnějším autentizačním prostředkem.
- NFC token: Metoda, jejíž bezpečnost záleží na konkrétním čipu obsaženém v tokenu. Může se tedy jednat o stejnou bezpečnost jako u FIDO tokenu nebo u čipových karet.

(2) UX testování a rozhovory s uživateli

Cílem rozhovorů s uživateli a UX testování bylo zjistit detailní hodnocení aplikace a testovaných autentizačních metod na vzorku vybraných koncových uživatelů. Tato studie byla nezbytná k otestování vzhledu a srozumitelnosti aplikací a zajištění jejich maximální uživatelské přívětivosti. Studii jsme provedli na vzorku 33 uživatelů všech věkových kategorií. Metodologický postup této studie je popsán detailně dále. Detailní výsledky tohoto testování jsou popsány zde.

Klíčová zjištění: UX testování

Mezi nejzásadnější zjištění UX testování patří následující:

- Konzistence ovládacích prvků i pojmenování je zásadní pro snadnou orientaci v aplikacích. Zmatení u uživatelů často vyvolává trojice *uživatelské*, *přihlašovací* a *klientské* jméno.
- Text v aplikacích by měl stručně a výstižně uživatele informovat o tom, co se právě odehrává. Toho lze docílit např. zvýrazněním klíčových slov a zkrácením dlouhých textů s příliš mnoha detaily, které odrazují od čtení.
- Animace použité v aplikacích jsou nápomocné, měly by co nejvíce odpovídat realitě (např. reálnému vzhledu použitého tokenu).
- V aplikacích byly použity nezvyklé či odborné koncepty, protože se jednalo o nová bezpečnostní řešení. Například použití 5místného PINu (na rozdíl od běžnějšího 4místného) bylo problematické, proto byl uživatel na jeho délku v aplikaci upozorněn. Označení FIDO a NFC token bylo také matoucí, proto bylo později používáno pouze slovo *token* s ukázkou tohoto hardwaru. Pojem *transakce* znamenající jakoukoliv operaci, kterou je třeba autentizovat, byl pro uživatele rovněž nejasný, protože tím rozuměli pouze finanční transakci. Nakonec bylo zvoleno označení *požadavek*.

Klíčová zjištění: Rozhovory s uživateli týkající se hodnocení autentizačních metod

Mezi hlavní doporučení pro vývoj a zavádění autentizačních metod z rozhovorů s uživateli, které se týkaly hodnocení autentizačních metod, patří následující:

- Nové metody autentizace by měly být nabízeny jako komplexní služba se zapojením relevantních institucí (např. bank) a služeb (např. podpora uživatele při útoku).
- Vydavatel autentizační metody musí chápat potřeby a obavy uživatele a brát na ně ohled při návrhu této metody.
- Při vývoji nových metod a kombinací je vhodné hledat takové, které využijí již stávající metody a pro uživatele běžně dostupná zařízení.
- Případné nové metody by mohly být využity pro více úkonů i mimo mobilní bankovnictví, aby se zvýšila jejich užitečnost a přijatelnost pro uživatele (např. token jako paměťový disk).
- S ohledem na relativní stálost preferencí autentizačních metod lze doporučit soustavně sledovat stav útoků, resp. bezpečnosti preferovaných metod a bezpečnostní řešení neustále vylepšovat.

Proč uživatelé preferují otisk prstu (co říkali v rozhovorech):

- Uživatelé věří, že každý otisk prstu je na celém světě jedinečný.
- Možná rizika jako únos či useknutí prstu jsou vnímaná jako nepravděpodobná, proto se jich uživatelé příliš neobávají.
- Z pohledu uživatelů není při používání otisku prstu třeba žádné speciální bezpečnostní chování.
- Otisk prstu je dnes podporován většinou chytrých telefonů. Uživatelé proto věří v budoucnost této metody, což snižuje jejich motivaci přijímat jiné nové technologie.
- Při této autentizační metodě uživatelé nepotřebují žádná další zařízení, je to rychlé, jednoduché a intuitivní. V případě nemožnosti použití je vždy k dispozici záložní metoda (obvykle PIN).

(3) **Kvantitativní šetření dospělé a stárnoucí populace**

Cílem kvantitativního šetření bylo zjištění aktuálních zkušeností s online bankovnictvím a otestování vybraných autentizačních metod (PINu, otisku prstu, NFC tokenu a platební karty vkládané do čtečky karet) se zaměřením na vnímanou uživatelskou přívětivost a bezpečnost a preferenci těchto metod. Kvantitativní šetření na vzorku 500 uživatelů (250 dospělých do věku 54 let, dále „dospělí", a 250 osob ve věku 55 a starších, dále „stárnoucí") navazovalo na UX testování a rozhovory s uživateli. Metodologický postup kvantitativní studie je detailně popsán dále. Detailní výsledky šetření jsou popsány zde.

Klíčová zjištění: Kvantitativní šetření

Zkušenosti s online bankovnictvím a autentizačními metodami (detailní výsledky zde)

- Naprostá většina respondentů využívala nějakou formu online bankovnictví (97 % dospělých, 86 % stárnoucích).
    - Nejčastěji měli internetové bankovnictví na počítači, především v případě dospělých pak používali i aplikace mobilního bankovnictví.
    - Obě populace přistupovaly do internetového bankovnictví nejčastěji několikrát měsíčně nebo několikrát týdně, ale málokdo denně.
- Autentizační metody pro přihlášení do bankovnictví, se kterými mělo zkušenost nejvíce uživatelů, byly přihlašovací jméno a heslo (shodně 87-88 %) a PIN (73 % dospělých, 76 % stárnoucích). s otiskem prstu měli častěji zkušenost dospělí (29 %) než stárnoucí (12 %).
- Při potvrzení plateb v online bankovnictví mělo nejvíce respondentů zkušenost s SMS kódem (přes 95 %) a následně PINem a heslem, se kterými měla zkušenost polovina dospělých a 36-39 % stárnoucích.

Dvoufaktorová autentizace (2FA) (detailní výsledky zde)

- Většina dotazovaných (84 %) s 2FA měla již předchozí zkušenost.
- Alespoň tři čtvrtiny uživatelů uvedly, že by 2FA chtěly používat pro placení kartou online a pro potvrzování převodu peněz v online bankovnictví. Pravděpodobně si tedy uvědomují důležitost ochrany aktiv a sami oceňují takové bezpečnostní prvky.
- Přestože s SMS kódem měli zkušenost téměř všichni respondenti, více jak polovině by nevadilo, kdyby byla tato metoda nahrazena jinou. Nahrazení SMS kódu by vadilo přibližně třetině populace. Předchozí zkušenost tedy nemusí nutně znamenat preferenci této metody.

Hodnocení testovaných autentizačních metod (detailní výsledky zde)

Na základě vyzkoušení autentizačních metod na chytrém telefonu je respondenti hodnotili v kategoriích *jednoduchost používání*, *praktičnost* a *bezpečnost*.

- Respondenti vnímali jednotlivé metody (otisk prstu, PIN, token a vložení platební karty do čtečky) převážně pozitivně ve všech třech kategoriích.
- Otisk prstu byl vnímán jako nejjednodušší, nejpraktičtější a zároveň nejvíce bezpečná metoda oběma populacemi.
- Stárnoucí hodnotili autentizační metody založené na vlastnictví předmětu (token a vložení karty do čtečky) podobně ve všech kategoriích. Naproti tomu dospělí vnímali vložení karty do čtečky jako složitější a méně praktické než použití tokenu.

Preference autentizačních metod pro potvrzování plateb (detailní výsledky zde)

Ptali jsme se také na preference jednotlivých autentizačních metod a jejich kombinací pro platby v online bankovnictví v závislosti na výši částky dané transakce:

- Otisk prstu by chtěla téměř polovina respondentů používat i pro potvrzení plateb o vyšších částkách, což je v souladu s jeho pozitivním hodnocením (jednoduchost, praktičnost a bezpečnost).
- Druhou nejvíce preferovanou jednofaktorovou metodou pro placení nižších i vyšších částek byl PIN, který měl hned po otisku prstu nejlepší hodnocení jednoduchosti a praktičnosti.
- V případě navrhovaných dvoufaktorových kombinací by přibližně pětina osob nikdy nechtěla jednotlivé kombinace používat. To je však patrně dáno preferencí jiné kombinace metod.
- Nadpoloviční většina respondentů (51-72 %) by chtěla jednotlivé 2FA kombinace metod používat pro potvrzování plateb o vyšších částkách.
- V populaci dospělých i stárnoucích byla mírně preferovaná 2FA kombinace využívající otisku prstu, tj. otisk prstu + token.

Shrnutí

Z provedených testování s uživateli se zaměřením na hodnocení autentizačních metod (otisk, PIN, token, vložení karty do čtečky) vyplynula jasná preference otisku prstu. Ten byl našimi respondenty hodnocen jako nejjednodušší na používání, nejpraktičtější i nejbezpečnější. Důvody naznačují mimo jiné rozhovory s uživateli. Uživatelé vnímají otisk jako jedinečný, a proto těžko zneužitelný (fyzická rizika vnímají jako nepravděpodobná). Dále pozitivně hodnotí současné rozšíření této metody a přítomnost záložní metody v případě nemožnosti použití.

Vzhledem ke stálosti vnímání a preferenci autentizačních metod lze mimo jiné doporučit, aby se usilovalo i o zvýšení bezpečnosti metod, které uživatelé preferují, tedy např. bezpečnější implementaci čteček otisků prstů.

Ačkoliv ostatní testované metody byly hodnoceny jako méně praktické (především ty založené na vlastnictví dalšího předmětu, tj. token a čtečka), jejich hodnocení bylo celkově stále pozitivní.

Tuto technickou zprávu citujte následovně:

Kružíková, A., Knapová, L., Gabrhelík, O., Šmahel, D., Dědková, L., Matyáš, V., Doležal, P., & Šmahelová, M. (2020). Uživatelské testování autentizačních metod mobilního bankovnictví: UX testování, rozhovory s uživateli a kvantitativní šetření. Brno: Masarykova univerzita.

TECHNICKÁ ZPRÁVA

(1) Bezpečnost a hrozby vybraných autentizačních metod: technická specifikace

Autentizace je proces, při kterém se ověřuje, zda je uživatel tím, za koho se vydává. Mezi nejznámější metody autentizace patří například přihlášení pomocí uživatelského jména a hesla. S rostoucím množstvím různých online služeb a zařízení stoupá i počet autentizací, které musí běžný uživatel denně provést. Dobrá použitelnost autentizačních metod je klíčovým aspektem pro jejich správné, bezproblémové a bezpečné využití. V této zprávě jsou diskutováni konkrétní zástupci jednofaktorové a dvoufaktorové autentizace. Při jednofaktorové autentizaci (dále „1FA“) se používá pouze jedna autentizační metoda jakožto jeden samostatný faktor (např. samostatný číselný kód), při dvoufaktorové autentizaci (dále „2FA“) se používá kombinace dvou nezávislých metod autentizace. Často se jedná o kombinaci různých typů metod: „něco, co mám“ – token; „něco, co znám“ – číselný kód/heslo; „něco, co jsem“ – biometrika.

Mezi nejvíce rozšířené autentizační metody bankovního sektoru patří číselný kód (PIN) nebo otisk prstu a jednorázový SMS kód. Přestože některé z těchto metod byly dlouhou dobu považovány za těžko napadnutelné, jejich bezpečnost nemusí být dostačující pro některé finanční operace (např. převod vyšších částek mezi účty).

Po vzájemném dialogu bezpečnostních expertů z firmy AHEAD iTec, s.r.o. a výzkumníků z oblasti počítačové bezpečnosti a psychologie Masarykovy univerzity byly pro použití na chytrých telefonech implementovány následující metody jako funkcionalita mobilní autentizační aplikace:

1. jednorázový SMS kód,
2. číselný kód (pětimístný PIN),
3. biometrika (otisk prstu),
4. hardwarový token (FIDO token, NFC token),
5. identifikační karta s čipem (vložení karty do čtečky nebo přiložení k NFC čtečce na telefonu).

Metody byly voleny mimo jiné s ohledem na pokrytí různých typů metod. Cílem bylo porovnat různě bezpečné metody a zahrnout i takové, které zatím nejsou příliš rozšířené, ale mají velký potenciál pro budoucí použití u různých skupin uživatelů pro zajištění větší bezpečnosti.

SMS kód

SMS kód je zatím stále nejčastěji používanou metodou v rámci dvoufaktorové autentizace pro většinu českých bank. Důvodem k rozšíření této metody byla expanze mobilních telefonů (nejen chytrých telefonů). Hlavní konkurencí SMS kódů byly OTP (One-Time Password) kalkulačky a další specializovaný hardware, který však představuje vysoké počáteční náklady. Další výhodou SMS kódů byla relativně jednoduchá implementace do systémů bank. Nevýhodou je pak cena za odeslanou SMS a bezpečnost této technologie. Útoky na bankovní účty pomocí přesměrování autentizační SMS směrem k útočníkovi jsou pro všechny banky dobře známé a i v ČR poměrně časté (byť nejsou příliš medializované). Útok spočívá v instalaci aplikace, která příchozí SMS z banky v reálném čase odešle na telefonní číslo útočníka. Platforma Android umožňuje vývoj i distribuci takových aplikací.

Číselný PIN

Útoky na PIN jsou obecně známé a v nejčastějších případech velmi jednoduché. Odchytit PIN lze několika způsoby:

- Vizuálním odpozorování (s*houlder surfing)* při zadávání, případně odpozorování ze stop na skle displeje telefonu.
- Pomocí sociálního inženýrství (např. phishingový e-mail).
- Pomocí útoku překrytím (uživatel zadá údaje do podvodné aplikace, která se vydává za oficiální službu).
- Útokem hrubou silou (*brute force*) na PIN (vyzkoušení všech možných kombinací), případně jeho odhadnutí.
- Pomocí keyloggeru (program zaznamenávající stisknuté klávesy na klávesnici).
- Vyčtení PINu z paměti zařízení, případně odchycením nebo odposlouchávánim komunikace.

Pokud ale dojde ke kompromitaci PINu, je možné jej změnit. Některým z výše uvedených útoků je možné se bránit dobře zvoleným PINem a jeho uložením v šifrované či hašované podobě.

Otisk prstu

Otisk prstu řeší některé potíže předchozích způsobů autentizace a úroveň zabezpečení je pro většinu případů užití dostatečná. Další výhodou je také rychlost, cena a uživatelská použitelnost. Přesto i tato technologie má své slabiny, proto je vhodná spíše jako doplňková metoda:

- Nepříliš dobrá hardwarová i softwarová implementace na zařízení s operačním systémem Android (zejména u levnějších modelů, ale taky na některých high-end telefonech) (Paul & Irvine, 2016).
- Absence kontroly živosti (tzn. čtečka otisků prstů není schopna rozeznat, jestli se jedná o prst živého člověka, nebo o jeho padělek; týká se platformy Android i iOS).
- Masterprint útoky (otisk prstu, který je podobný více otiskům prstů – tento útok je možný, protože při autentizaci se neporovnává celý otisk, ale pouze některé body).

FIDO token

Bezpečnostní koncept FIDO tokenů je založen na silné asymetrické kryptografii využívající technologii eliptických křivek (ECDSA). Každý výrobce HW podporující FIDO protokol musí splňovat náročné certifikace na ochranu privátních klíčů generovaných a uložených přímo v tokenu, čímž se výrazně eliminuje možnost vyzrazení klíče. Pro banky a další podobné subjekty je však otevřenost celého řešení zatím zásadní problém bránící jejímu širšímu použití pro koncové klienty. FIDO protokol umožňuje uložení libovolných klíčů na libovolný FIDO token a banka tedy z definice nemůže mít žádnou kontrolu nad tím, kdo vlastní fyzický token, případně k jakým dalším službám je token využíván.

Pro podporu FIDO tokenů bylo nutné implementovat oficiální SDK (Software Development Kit) pro Android, které se v rámci vývoje i následného testování ukázalo jako nevhodné jak z pohledu stability aplikace, tak z pohledu uživatelského rozhraní. SDK totiž obsahuje vizuální komponenty, které byly pro uživatele matoucí a které nebylo možné změnit či nepoužít.

Obrázek 1: Hardware používaný při testování (chytrý telefon, NFC token, čtečka čipových karet a platební karta).

Čipová karta

Bezpečnost čipových karet je vždy závislá na samotné implementaci autentizačních funkcí, na použitých algoritmech, kryptografii a parametrech klíčů (Mayes & Markantonakis, 2017). Nicméně obecně platí, že čipové karty jsou nejsilnějším prostředkem k autentizaci. Použitím asymetrických algoritmů (ECDSA, RSA) v kombinaci se správně nastavenými procesy čipových karet (personalizace, distribuce, aktivace, nastavení PINu apod.) vznikají ekosystémy využitelné v prostředích s nejvyššími nároky na bezpečnost.

Použití těchto systémů v kombinaci s mobilními telefony však zatím stále vázne, proto byly v rámci projektu zkoumány dva způsoby využití čipové karty v komunikaci s telefonem:

1. Bezkontaktní čipová karta komunikující pomocí NFC technologie.
2. Kontaktní čipová karta vložená do externí čtečky karet komunikující přes Bluetooth technologii.[1]

Samotná bezpečnost je v těchto případech srovnatelná, obě karty obsahují stejné algoritmy, stejně velké klíče, stejný typ technologie čipu. Jak technologie Bluetooth, tak NFC může být odposlouchávána, případně modifikována. Rozdíl v bezpečnosti pak vzniká při (ne)využití a délce PINu.

NFC token

NFC token může obsahovat několik typů čipu, a to jak čipy kompatibilní s FIDO protokolem, tak i čipy odpovídající klasickým čipovým kartám zmíněným v předchozí části. Dále existuje spousta proprietárních NFC čipů obsahujících symetrickou a/nebo asymetrickou kryptografii (Mayes & Markantonakis, 2017). Pro naši implementaci jsme zvolili NTAG[2] čip od společnosti NXP. Tento čip je designovaný tak, aby co nejlépe podporoval komunikaci s mobilním telefonem a splňoval základní požadavky na bezpečnost. Samotná bezpečnost tohoto řešení nedosahuje úrovně čipových karet, je založena na ověření originality tokenu pomocí eliptických křivek (ECC).[3]

[1] Pro komunikaci s platební kartou byla zvolena čtečka kontaktních čipových karet ACS (ACR3901U-S1), ACS SDK bylo implementováno jako součást mobilní autentizační aplikace.
[2] Detailní popis zde: https://www.nxp.com/products/rfid-nfc/nfc-hf/ntag:MC_71717
[3] Detailní popis zde: https://www.nxp.com/products/rfid-nfc/nfc-hf/ntag/ntag-for-tags-labels/ntag210-ntag212-ntag-21x-nfc-forum-type-2-tag-ic-with-multiple-user-memory-sizes:NTAG210_NTAG212#documentation

(2) UX testování a rozhovory s uživateli

Metodologie

Popis studie

UX testování a rozhovory s uživateli spočívaly v iterativním testování prototypů autentizačních metod a jednotlivých aplikací na vybraných reprezentantech cílové skupiny, aplikaci získaných poznatků na testovaný software a jejich následné úpravě a inovaci. Primární testovanou aplikací byla digitální identita IDport sloužící pro autentizaci uživatele a autorizaci požadavků, podporující jednotlivé autentizační metody. Uživatelé dále interagovali s fiktivním online bankovnictvím YourBank (mobilní aplikace a webové rozhraní).

Proběhla 4 samostatná kola testování, po každém kole byla pak realizována implementace výsledných zjištění do příslušného softwaru. Takové iterativní testování a vývoj zajistilo potřebnou kvalitu autentizačních metod, aby mohly být otestovány s více uživateli v rozsáhlém kvantitativním šetření. První a druhé kolo zahrnovalo především UX testování. Třetí a čtvrté kolo cílilo především na detailní zhodnocení autentizačních metod, jejich vnímané přívětivosti a bezpečnosti a způsobu uvažování o těchto tématech. Vedle PINu a otisku prstu byly v jednotlivých kolech testovány následující metody:

1. kolo: jednorázový SMS kód, hardware token (FIDO token) a platební karta vkládaná do čtečky karet.

2. kolo: hardware token (FIDO token) a platební karta vkládaná do čtečky karet.

3. kolo: hardware token (NFC token) a platební karta vkládaná do čtečky karet.

4. kolo: platební karta (načtená telefonem přes NFC).

Změna autentizačních metod mezi jednotlivými koly (např. přechod od FIDO tokenu k NFC tokenu) byla způsobena technickými aspekty a uživatelským hodnocením jednotlivých metod. V případě FIDO tokenu bylo nutné přesměrování na externí službu, u které nebylo možné zajistit stabilní průběh autentizačního procesu pro všechny uživatele. Navíc i samotní uživatelé hodnotili externí službu jako problematickou a uživatelsky nepřívětivou. FIDO token jsme se proto rozhodli dále netestovat a nahradit ho tokenem komunikujícím s telefonem na bázi NFC.

Postup testování

Uživatel si při testování vyzkoušel alespoň tři samostatné metody autentizace a absolvoval rozhovor o uživatelské přívětivosti, preferencích a vnímání bezpečnosti metod a vyplnil dotazníky (demografické údaje a přívětivost metod). Celý postup s jedním účastníkem trval od 45 minut do 90 minut. Před samotným testováním respondent podepsal informovaný souhlas. Testování bylo schváleno *Etickou komisí pro výzkum* Masarykovy univerzity.

Na začátku testování byla účastníkovi popsána situace, že mu jeho banka doporučila používat novou aplikaci pro potvrzování požadavků v bankovnictví (tj. mobilní autentizační aplikaci). Uživatel si měl aplikaci aktivovat a následně se přihlásit do bankovnictví a případně zaplatit za dovolenou. V obou případech byl uživatel z online bankovnictví přesměrován do autentizační aplikace pro potvrzení požadavku.

V rámci testování si účastníci vyzkoušeli aktivační a autentizační scénář. Aktivační scénář (aktivace autentizační aplikace, resp. potvrzení identity) využíval metody zaslání jednorázového SMS kódu, použití identifikační karty s čipem (platební karta vkládaná do čtečky karet) nebo hardwarového tokenu (FIDO nebo NFC). Autentizační scénář (potvrzování přihlášení do bankovnictví a odeslání platby) využíval PIN nebo otisk prstu a vložení platební karty do čtečky karet nebo hardwarový token (FIDO nebo NFC).

Vzorek a jeho výběr

Uživatelská studie cílila na dospělé osoby včetně starší populace a seniorů. Podmínkou účasti bylo aktivní používání chytrého telefonu a internetového bankovnictví a studium a práce mimo oblast IT.

Výběr vzorku byl příležitostný s využitím metody sněhové koule (doporučení dalších osob od samotných účastníků).

Celkem bylo v rámci uživatelské studie otestováno 33 uživatelů: 8 v prvním kole, 8 ve druhém kole, 7 ve třetím kole a 10 ve čtvrtém kole. Z celkového počtu 33 účastníků bylo 17 žen a 12 účastníků starších 60 let.

Výsledky a doporučení z UX testování a rozhovorů s uživateli

UX testování pomocí průchodů aplikacemi hodnotilo uživatelskou přívětivost a spokojenost uživatelů. Rozhovory s uživateli byly zaměřeny na to, jak uživatelé uvažují nad bezpečností a podle čeho se rozhodují.

UX testování

V prvních dvou kolech testování byl kladen důraz především na estetiku a srozumitelnost vizuálních a textových prvků.

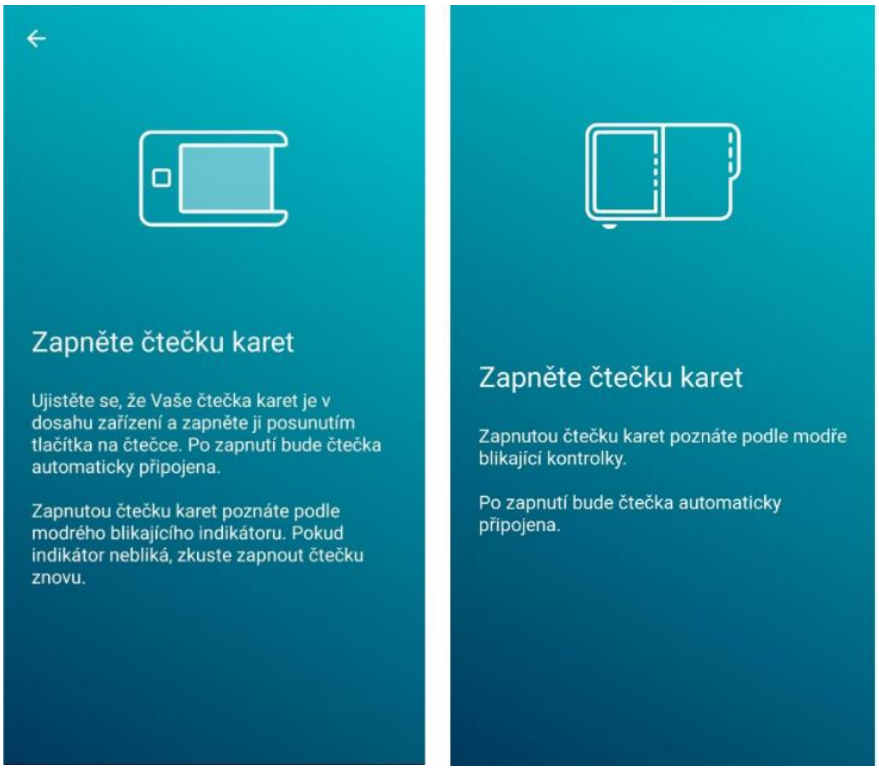
Konzistence

Přestože průchod aplikacemi byl poměrně krátký, uživatelé si rychle vytvořili návyk a pokud se aplikace v některé části lišila (např. na jedné obrazovce byl popisek v horní části a na jiné obrazovce v části dolní), vnímali to jako matoucí. Je třeba dbát i na konzistenci pojmenovávání. Uživatelům dělalo největší potíže *uživatelské* jméno, které bylo v dopise od banky označeno jako *klientské* jméno. Uživatelé u této nesrovnalosti zmiňovali i existenci *přihlašovacího* jména (které nebylo v rámci testování nikde uvedeno) a fakt, že různé služby používají tyto tři termíny v různých významech. Také si nebyli jistí, jestli se jedná o synonyma. V pozdějších verzích aplikací a testovacích materiálů byl konzistentně použit pouze termín *klientské jméno*, což už nezpůsobovalo žádné problémy.

Množství textu

Uživatelé komentovali množství vysvětlujícího textu v aplikaci. Obecně chtějí mít přehled o tom, co se právě odehrává, protože chtějí mít aplikaci a proces placení pod kontrolou, ale příliš dlouhé texty je spíše odrazují od čtení. Do pozdějších verzí aplikace byly texty reformulovány, aby byly krátké, ale výstižné. Informace, které uživatelé nepovažovali za příliš přínosné, byly vypuštěny a klíčová slova byla zvýrazněna tučným písmem. Například namísto *„PIN budete používat ve Vašem e-bankovnictví. Nepoužívejte tedy osobní nebo snadno uhodnutelná data”* bylo použito *„**Osobním PINem** budete potvrzovat příchozí požadavky. Nepoužívejte snadno uhodnutelná čísla.”* Dalším příkladem změny je nahrazení *textu „Vaše zařízení splňuje podmínky pro potvrzování operací pomocí otisku prstu. Otisk prstu můžete využívat místo*

Vámi zvoleného PIN kódu. Pro pokračování v aplikaci přiložte ukazováček na čtečku otisku prstů" textem *„Pro dokončení aktivace ověřte svoji identitu pomocí otisku prstu."* Další příklad je viditelný na Obrázku 2.



Obrázek 2: Úprava obrazovky na základě iterativního testování (zkrácení textu a realistická animace).

Animace odpovídající realitě

Autentizační aplikace obsahovala animace, které znázorňovaly použití inovativních testovaných autentizačních metod, např. stisknutí tlačítka na FIDO tokenu, přiložení NFC tokenu/NFC platební karty k telefonu, zapnutí čtečky karet a následné vložení platební karty do čtečky (viz Obrázek 2). Tyto animace sloužily jako nápověda, protože většina uživatelů se s těmito metodami setkala při testování poprvé. Zpětná vazba ukázala, že použití animací je nápomocné, nicméně je důležité, aby animace co nejvíce odpovídaly realitě (např. bylo důležité, aby ikona znázorňující čtečku karet co nejvíce odpovídala vzhledu čtečky používané při testování, příliš velké zjednodušení ikony nebylo pro respondenty pochopitelné).

Zástupci stárnoucí populace měli často problém s přiložením prstu na čtečku otisků prstů, protože namísto na čtečku, která jim byla předtím předvedena, přikládali prst na displej, kde jim ikona připomínala tlačítko. Nejlépe fungující řešení po několika iteracích vylepšování je vyobrazeno na Obrázku 3.

Obrázek 3: Výzva pro přiložení prstu na čtečku otisků prstů.

Nezvyklé či odborné koncepty

Uživatelé se v rámci testování setkali s několika ne příliš obvyklými koncepty, které jim dělaly problémy. Prvním příkladem je volba 5místného PINu namísto obvyklejšího 4místného. Uživatelé tím byli překvapeni, a především starší uživatelé měli potíže se zadáním 5 číslic (ať už z důvodu nepovšimnutí, že mají zadat ještě jednu číslici, nebo proto, že vymyslet 5 čísel pro ně bylo složitější než vymyslet pouze 4). Uživatelé také vyjádřili obavy nad zapamatovatelností o jedno číslo delšího PINu, ale zároveň jej hodnotili jako bezpečnější.

Dalším novým konceptem bylo použití hardware tokenů: *FIDO* a *NFC tokenů*. Především stárnoucí uživatelé měli problémy se zapamatováním slova *token*. *FIDO* a *NFC* bylo matoucí pro většinu uživatelů, protože nevěděli, co si pod těmito zkratkami představit. V pozdějších fázích, kdy se již dále netestoval *FIDO token,* ale pouze *NFC token* bylo používáno pouze označení *token* spolu s demonstrací tohoto hardwaru.

Autentizační aplikace IDport je v zásadě univerzální aplikace pro potvrzování různorodých akcí. Pojmenování těchto akcí vyžadovalo několik návrhů a jejich iterativní vylepšování. z technických důvodů nebylo možné pojmenovat každou akci jinak, např. *přihlášení*, *finanční transakce* apod. Pod pojmem *transakce* ale uživatelé rozuměli finanční transakci a nutnost potvrdit *transakci* přihlášení tak pro ně byla matoucí. Nakonec jsme zvolili označení *požadavek*, stále jej ale nepovažujeme za nejvhodnější pojmenování.

Rozhovory s uživateli

Rozhovory s uživateli se týkaly především toho, jak uživatelé uvažují nad bezpečností autentizačních metod, a podle čeho se rozhodují, zda chtějí danou metodu používat.

V prvních třech kolech jsme při testování autentizace pomocí hardwarového tokenu nebo čtečky platebních karet zjistili, že uživatelé mají velké výhrady k vlastnictví dalšího zařízení, které se zdá z pohledu uživatele jako neužitečné (což by bylo možné vyřešit rozšířením použití takového zařízení). Jako důvody uváděli zejména nepraktičnost vlastnictví další věci a riziko ztráty. Rozhodli jsme se proto připravit uživatelské testování s NFC platební kartou, tedy v současné chvíli běžnou platební kartou, kterou uživatelé dostávají k bankovním účtům.

Při porovnání autentizačních metod dělají uživatelé poměrně komplexní rozhodnutí, zvažují mnoho různých souvislostí a nehodnotí bezpečnost metody jen podle technických parametrů. Uživatelskou použitelnost pro ně nedefinuje pouze to, jak se chová samotná metoda nebo aplikace, ale např. i její potenciální rozšíření nebo uživatelská podpora při selhání. Z hlediska bezpečnosti zvažují jednotlivé komponenty, jejich spolehlivost a možnost záložních řešení. Jedním z důvodů, proč otisk prstu v hodnocení uživatelů předčil bezkontaktní platební kartu, bylo to, že uživatelé vnímají otisk v kontextu dosavadního užívání dohromady s PIN kódem a zároveň vědí, co mají dělat, pokud některá z jim známých metod nefunguje. U karty tyto krizové scénáře neznali, což snižovalo subjektivně vnímanou bezpečnost a použitelnost. Obdobně pro ně bylo důležité vědět, kdo nese za rizika odpovědnost a kdo bude případné bezpečnostní obtíže (např. odcizení karty) řešit. Bezpečnost pro uživatele nesymbolizuje jen samotné technické řešení, ale i instituce, služby a další aktéři, kteří tato řešení doprovázejí.

Otisk prstu byl hodnocen jako uživatelsky přívětivý díky své rychlosti a pohotovosti, ale zároveň uživatelům přišel i bezpečný díky své unikátnosti a tomu, že jej nelze jednoduše odcizit nebo ztratit. V případě využití platebních karet se uživatelé obávali, že s nimi nejsou fyzicky spojeny, že je někdo může odcizit společně s telefonem nebo že může pohledem zachytit a zneužít údaje, které jsou na nich napsány. Uživatelé ovšem nereflektovali, že bezkontaktní platební kartu používají běžně pro platbu v obchodech, a nikdo nezmínil, že by se při těchto činnostech obával stejných rizik.

Uživatelé ve svém hodnocení, a dost možná i v bezpečnostním chování, vycházeli z představy, která zdůrazňuje fyzické hrozby, jako je např. krádež. Tento model je ale nepřesný a neumožňuje jim adekvátně zhodnotit digitální hrozby, i když je může motivovat k bezpečnějšímu chování, například k provádění transakcí na neveřejném místě. Přestože tato představa je nepřesná, ovlivňuje ochotu uživatelů používat jednotlivé autentizační metody. Proto je důležité, aby vydavatelé autentizačních metod těmto představám rozuměli a při návrhu je brali v potaz.

Informace výše vychází z našich analýz a částečně z našeho článku *„Jak uživatelé přemýšlejí o bezpečnosti v kontextu mobilního bankovnictví?”* publikovaném v časopise Data Security Management 2/2019 (Doležal, Dařbujanová, & Knapová, 2019).

(3) Kvantitativní šetření dospělé a stárnoucí populace

Metodologie

Popis kvantitativního šetření

Cílem kvantitativního šetření bylo zjištění aktuálních zkušeností s online bankovnictvím a otestování vybraných autentizačních metod se zaměřením na vnímanou uživatelskou přívětivost a bezpečnost a preferenci těchto metod. Kvantitativní šetření na vzorku 500 uživatelů (250 dospělých do věku 54 let a 250 osob ve věku 55 a starších) navazovalo na UX testování a rozhovory s uživateli a získané poznatky.

Testované autentizační metody byly shodné se třetím kolem UX testování a rozhovorů s uživateli:

- PIN
- otisk prstu
- hardware token (NFC token)
- platební karta vkládaná do čtečky karet.

Primární testovanou aplikací byla opět aplikace digitální identity IDport sloužící pro autentizaci uživatele a autorizaci požadavků, podporující jednotlivé autentizační metody. Uživatelé dále interagovali s fiktivním online bankovnictvím YourBank.

V rámci přípravné fáze byla provedena série kroků k zajištění bezproblémového průběhu kvantitativního šetření. V první řadě byly implementovány změny v testovaných aplikacích (autentizační aplikace IDport a bankovnictví YourBank) na základě UX testování, které jsou popsány výše. Pro rozsáhlé standardizované testování autentizačních metod bylo dále nutné zajistit funkčnost a shodné chování všech testovacích scénářů i v případě chybějícího či špatného internetového připojení. Byla proto vytvořena nativní aplikace mobilního bankovnictví pro operační systém Android, která nevyžadovala připojení k internetu. V neposlední řadě byly upraveny tištěné testovací materiály používané v rámci testování. Zde se jednalo například o dopisy od banky popisující postup aktivace aplikace IDport (k nalezení v příloze zde), fiktivní fakturu k platbě, návody k zařízením (viz Obrázek 4). Stejně tak byl vytvořen vysoce standardizovaný postup testování a detailní školicí materiály pro tazatele.

Postup testování

Průběh testování a úkoly na chytrém telefonu vycházely ze zkušeností z UX testování a rozhovorů s uživateli. Testování v rámci kvantitativního šetření probíhalo individuálně (tazatel s jedním respondentem) a sestávalo z plnění úkolů na chytrém telefonu a vyplnění dotazníků. Celý postup s jedním uživatelem trval cca 30-90 min. Na začátku testování respondent podepsal informovaný souhlas. Testování bylo schváleno *Etickou komisí pro výzkum* Masarykovy univerzity.

Respondentům byla opět prezentována hypotetická situace, kdy jim jejich fiktivní banka YourBank doporučila používání mobilní autentizační aplikace IDport pro potvrzování požadavků v bankovnictví. Uživatel si měl aplikaci aktivovat a následně se přihlásit do bankovnictví a zaplatit za dovolenou. V obou případech byl uživatel z online bankovnictví přesměrován do autentizační aplikace pro potvrzení daného požadavku.

Obrázek 4: Standardizované rozložení materiálů pro scénář na chytrém telefonu s využitím čtečky karet.

V rámci testování si tak uživatel vyzkoušel aktivační a autentizační scénáře. V rámci aktivačního scénáře (aktivace autentizační aplikace IDport, resp. potvrzení identity) si nastavil a použil všechny testované autentizační metody. Následně prošel dvěma autentizačními scénáři: potvrzení přihlášení do bankovnictví YourBank a potvrzení odeslání platby. Při potvrzení přihlášení použil jeden faktor dle vlastních preferencí: PIN nebo otisku prstu. Odeslání platby bylo potvrzeno dvěma faktory v závislosti na variantě testovacího průchodu: (i) hardware tokenem a následně opět dle preference PINem nebo otiskem prstu, nebo (ii) vložením platební karty do čtečky karet a následně zadáním PINu k této kartě.

Průběh kvantitativního šetření byl následující (znázorněn také na Obrázku 5):

- Dotazník A (5-10 minut): Vyplňován před samotným testováním na chytrém telefonu. Pokrýval demografické otázky, sebehodnocení znalostí a dovedností s technologiemi, postoje k online bezpečnosti, bezpečné chování na chytrém telefonu.
- Testování na chytrém telefonu, varianta TOKEN: Aktivace aplikace IDport, přihlášení do bankovnictví YourBank a odeslání platby s využitím NFC tokenu, PINu a otisku prstu.

- Dotazník B1 (2 minuty): Kontrolní ohodnocení testování na chytrém telefonu bezprostředně po jeho skončení (snadnost, vnímaná délka, srozumitelnost instrukcí).
- Testování na chytrém telefonu, varianta ČTEČKA KARET: Aktivace aplikace IDport, přihlášení do bankovnictví YourBank a odeslání platby s využitím čtečky karet, PINu a otisku prstu.
- Dotazník B2 (2 minuty): Kontrolní ohodnocení testování na chytrém telefonu bezprostředně po jeho skončení (snadnost, vnímaná délka, srozumitelnost instrukcí).
- Dotazník C (15-20 minut)**:** Vyplňován po dokončení obou variant testování na chytrém telefonu. Obsahoval hodnocení vyzkoušených autentizačních metod z hlediska použitelnosti a bezpečnosti, preference autentizačních metod, dosavadní zkušenosti s autentizačními metodami a online bankovními službami, zkušenosti a preference dvoufaktorové autentizace.

Obrázek 5: Schéma postupu testování.

Vzorek a jeho výběr

Kvantitativní šetření bylo provedeno ve dvou nezávislých sběrech dat. První se zaměřil na dospělou populaci (dospělí do věku 54 let, N=250, dále „dospělí"), druhý sběr cílil na populaci stárnoucí (starší 55 let, N=250, dále „stárnoucí"). Podmínkou účasti bylo používání chytrého telefonu s operačním systémem Android, navíc zástupci stárnoucí populaci nesměli mít pracovní zkušenost nebo vzdělání v IT.

Šetření na dospělé populaci bylo provedeno profesionální agenturou FOCUS, která zajistila reprezentativní vzorek zkoumané populace s ohledem na pohlaví, věk, vzdělání, velikost sídla, kraj a socioekonomický status. Testování prováděli profesionální tazatelé.

Šetření na stárnoucí populaci koordinoval výzkumný tým Masarykovy univerzity. Pro sběr dat byli rekrutováni tazatelé především z řad studentů bakalářského a magisterského stupně. Sběr dat provádělo celkem 24 tazatelů, kteří byli výzkumným týmem detailně proškoleni a úspěšně provedli pilotní testovací sezení. Metoda výběru respondentů byla příležitostná; tazatelé oslovovali osoby v jejich okolí, byly kontaktovány různé seniorské organizace a spolky a studující univerzity třetího věku. Tento výběr byl doplněn metodou sněhové koule, tj. oslovení respondenti mohli sami doporučit a oslovit dalšího relevantního respondenta.

Popis vzorku dospělých osob

Ze vzorku 250 dospělých byly vyloučeny tři případy kvůli nízké kvalitě dat. Výsledný vzorek dospělých osob zahrnoval 247 osob do 54 let věku, 114 mužů (46 %) a 133 žen (54 %). Průměrný věk byl 38,75 let, medián 38 let, směrodatná odchylka 9,23.

Rozvrstvení vzorku podle vzdělání bylo následující: základní 4 %, středoškolské bez maturity 33 %, středoškolské s maturitou 30 %, vyšší odborné 5 %, vysokoškolské 29 %. (Pozn.: Vlivem zaokrouhlení se v některých případech celkový součet procent nemusí rovnat 100 %).

Rozvrstvení vzorku podle velikosti obce pobytu: do 1 999 obyvatel 18 %, 2 000-4 999 obyvatel 5 %, 5 000-9 999 obyvatel 7 %, 10 000-19 999 obyvatel 5 %, 20 000-49 999 obyvatel 9 %, 50 000-99 999 obyvatel 12 %, 100 000 a více obyvatel 45 %.

Hlavním zdrojem příjmu většiny dospělých respondentů do 54 let byla práce na plný úvazek (69 %), práce na částečný úvazek (9 %) či mateřská/rodičovská dovolená (11 %). Dále respondenti uváděli status studenta (3 %), nezaměstnaného (4 %) a důchod jako hlavní zdroj příjmu (1 %). Zbylí respondenti (2 %) nechtěli zdroj příjmu uvést.

Z dalších analýz je vyloučeno dalších 5 respondentů (všichni muži), protože se věnovali specificky tématu IT bezpečnosti a jejich data byla zkreslená oproti zbytku vzorku.

Popis vzorku stárnoucích osob

Výsledný vzorek stárnoucích osob zahrnoval 250 osob starších 55 let, 98 mužů (39 %) a 152 žen (61 %). Průměrný věk byl 62,58 let, medián 61 let, směrodatná odchylka 6,70.

Ve vzorku stárnoucích osob bylo vyšší zastoupení osob se středoškolským vzděláním s maturitou (42 %) a vysokoškolským vzděláním (41 %). Výrazně méně osob mělo vzdělání středoškolské bez maturity (9 %), vyšší odborné (5 %) či základní (3 %).

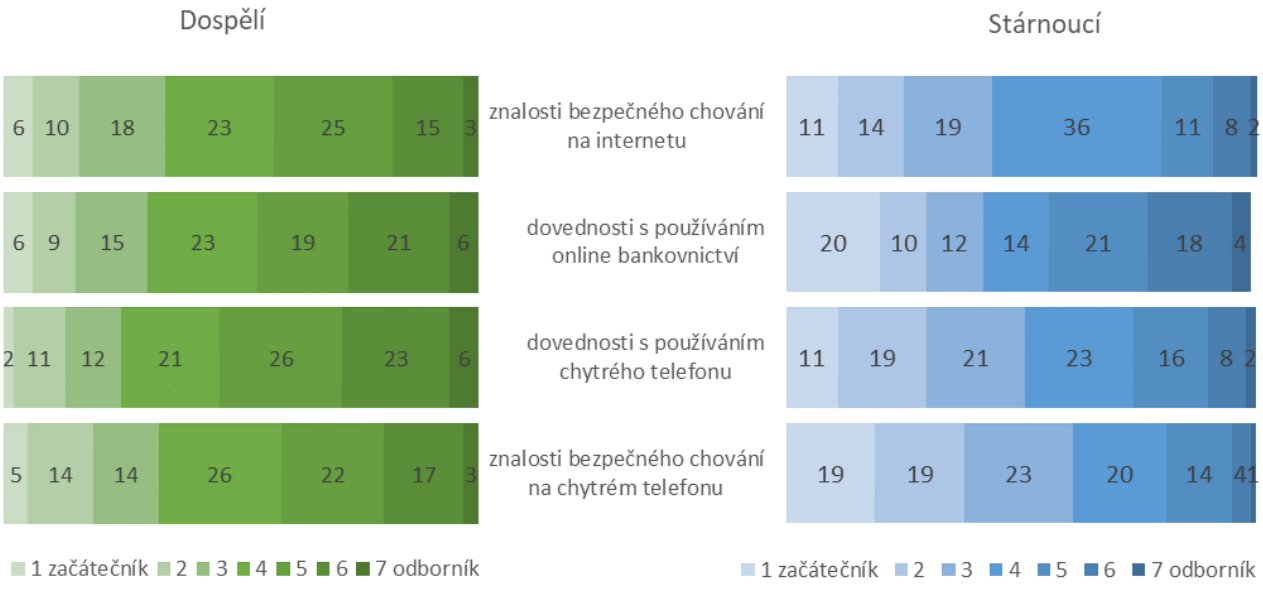
Pro polovinu respondentů (51 %) byla hlavním zdrojem příjmu práce na plný úvazek, pro 41 % důchod, pro 6 % práce na částečný úvazek. Zbylé osoby (1 %) byly nezaměstnané nebo nechtěly uvést hlavní zdroj příjmu.

Při interpretaci následujících analýz včetně porovnávání výsledků dospělých a stárnoucích osob je třeba brát v potaz, že vzorek dospělých je reprezentativní s ohledem na demografie ČR, zatímco u vzorku stárnoucích osob se jedná o příležitostný vzorek osob. Jelikož bylo podmínkou účasti používání chytrého telefonu s operačním systémem Android, jedná se ve vzorku osob starších 55 let pravděpodobně o technologicky zdatnější podskupinu stárnoucích.

Výsledky a doporučení z kvantitativního šetření

Následující výsledky vycházejí z dotazníkových odpovědí, vlivem zaokrouhlení se v některých případech celkový součet procent nemusí rovnat 100 %.

V první řadě hodnotili respondenti svoje znalosti bezpečného chování online a na chytrém telefonu, dovednosti s používáním online bankovnictví a dovednosti s používáním chytrého telefonu na škále od 1 – začátečník do 7 – odborník. Z Grafu 1 lze vyčíst, že zástupci dospělé populace hodnotili všechny své dotazované znalosti a dovednosti jako lepší než zástupci stárnoucí populace. Větší rozdíly jsou patrné například u hodnocení dovedností s mobilním bankovnictvím, kdy se 20 % stárnoucích označilo za úplné začátečníky (hodnota 1), zatímco mezi dospělými to bylo 6 %. Podobně tomu je v případě znalostí bezpečného chování na chytrém telefonu, které 19 % stárnoucích hodnotilo jako začátečnické (hodnota 1), a dalších 42 % jako spíše podprůměrné (hodnota 2 nebo 3). V případě dospělých do 54 let se ohledně bezpečného chování na chytrém telefonu za začátečníky považovalo 5 % respondentů, za spíše podprůměrné pak dalších 28 %.



Graf 1: Sebehodnocení vybraných znalostí a dovedností s technologiemi.

Zkušenosti s online bankovnictvím a autentizačními metodami

Naprostá většina dotazovaných v obou populacích měla účet v nějaké bance (97 % dospělých a 99 % stárnoucích) a většina také uvedla používání nějaké formy online bankovnictví (97 % dospělých a 86 % stárnoucích). Platební kartu ke svému účtu měli téměř všichni dospělí (98 %) i stárnoucí (97 %).

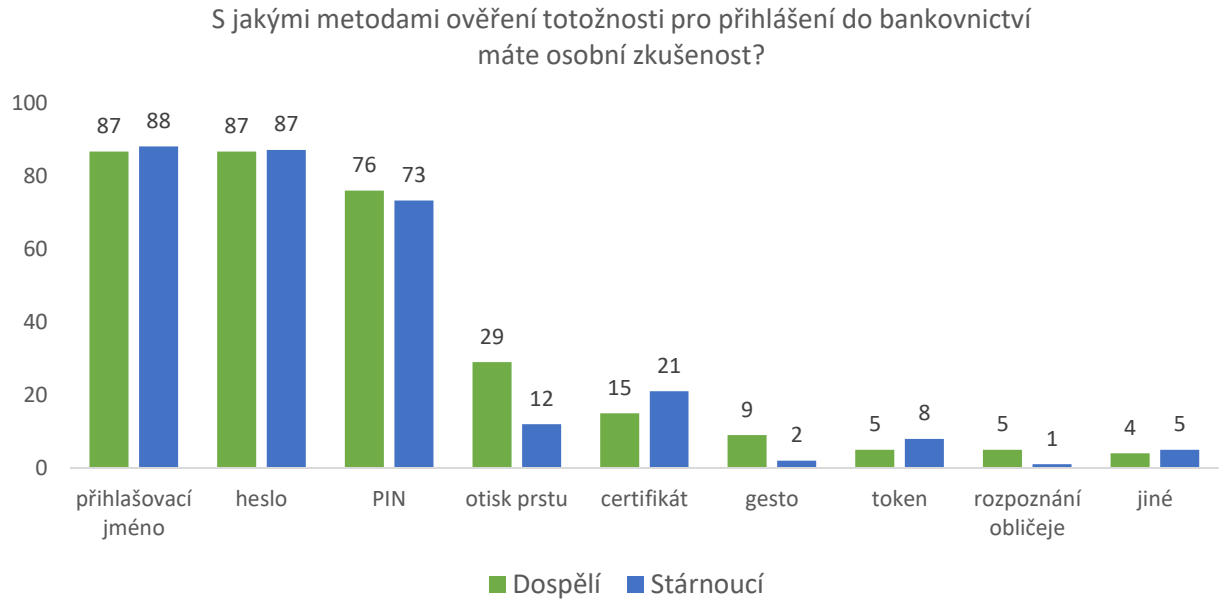
Nejčastěji používanou formou online bankovnictví bylo internetové bankovnictví na počítači, které používalo 81 % dospělých osob (resp. 84 % z těch, kteří používají nějakou formu online bankovnictví), a to po dobu průměrně 8,5 roku (směrodatná odchylka 4,5) a 84 % stárnoucích osob (resp. 98 % z těch, kteří používají nějakou formu online bankovnictví), průměrně 9,2 let (směrodatná odchylka 5,1 let). Dospělí a stárnoucí používali internetové bankovnictví na počítači podobně často, nejčastěji uváděli používání několikrát týdně (dospělí 33 %, stárnoucí 32 %) nebo několikrát měsíčně (dospělí 39 %, stárnoucí 43 %). Pouze 6 % dospělých a 7 % stárnoucích uživatelů uvedlo, že online bankovnictví na počítači používá každý den. Proto je třeba nabídnout takové autentizační metody, které budou schopni uživatelé používat opakovaně a zároveň i po delším časovém odstupu.

Používání aplikace mobilního bankovnictví na telefonu nebo tabletu uvedlo 52 % dospělých osob (resp. 54 % z těch, kteří používají nějakou formu online bankovnictví), a to po dobu průměrně 4,4 roku (směrodatná odchylka 2,9), zatímco mezi stárnoucími to bylo 30 % (resp. 35 % z těch, kteří používají nějakou formu online bankovnictví), průměrně 5 let (směrodatná odchylka 4,2 let).

Přistupování do online bankovnictví skrze prohlížeč v telefonu nebo tabletu uvedlo 20 % dospělých (resp. 21 % z těch, kteří používají nějakou formu online bankovnictví), a to po dobu průměrně 4,7 let (směrodatná odchylka 3,2), ze stárnoucích je to 11 % (resp. 13 % z těch, kteří používají nějakou formu online bankovnictví), průměrně 5,5 let (směrodatná odchylka 4,4 let).

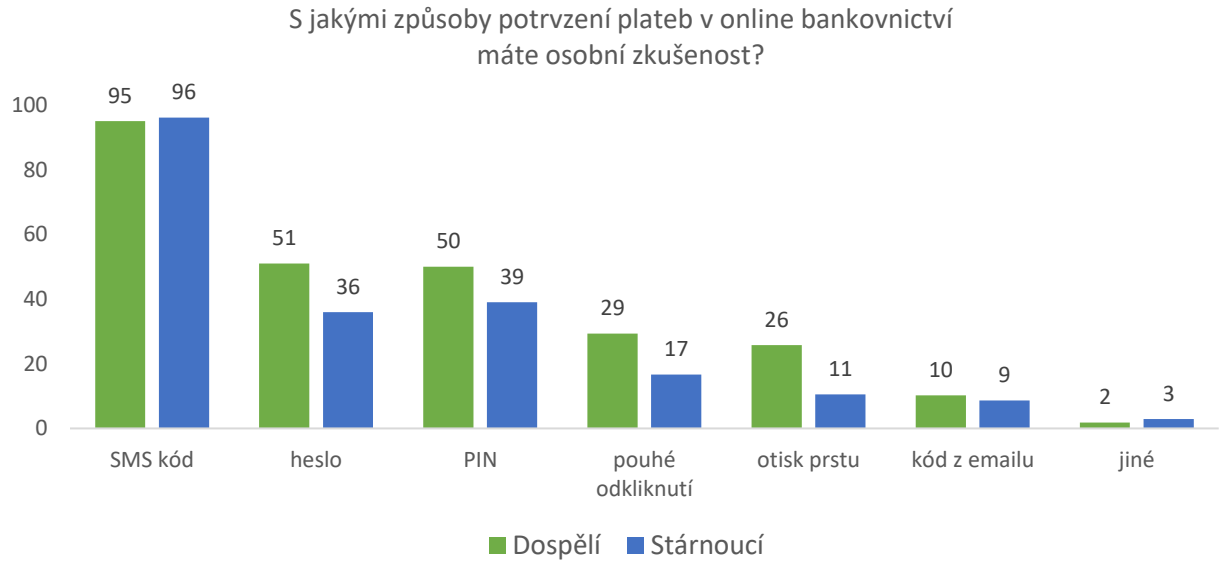
Nejvíce používanou formou online bankovnictví pro obě populace tedy bylo internetové bankovnictví na počítači, především mezi uživateli bankovnictví z řad stárnoucích používali online bankovnictví na počítači téměř všichni. Naopak online bankovnictví v chytrém telefonu či tabletu je dle našeho šetření spíše charakteristikou mladší věkové skupiny. Dospělých osob, které používaly bankovnictví v telefonu nebo tabletu (ať už ve formě aplikace nebo přes prohlížeč), byly dvě třetiny, což je přibližně dvakrát více než v případě stárnoucích.

Co se přihlášení do online bankovnictví týče, autentizační metody, se kterými mělo zkušenost nejvíce dospělých i stárnoucích uživatelů, jsou přihlašovací jméno (87 % dospělých, 88 % stárnoucích), heslo (87 % dospělých, 88 % stárnoucích) a PIN (76 % dospělých, 73 % stárnoucích), viz Graf 2. S výše uvedenými metodami měly obě populace zkušenost přibližně stejně často. Rozdíly jsou však například u otisku prstu, se kterým měli častěji zkušenosti dospělí (29 % dospělých, 12 % stárnoucích), certifikátu, se kterým měli naopak více zkušeností stárnoucí (15 % dospělých, 21 % stárnoucích), a gestu, které zkusilo jen několik stárnoucích (9 % dospělých, 2 % stárnoucích). To, že mají uživatelé s těmito metodami zkušenost, nutně neznamená, že je v současnosti používají nebo preferují. Zkušenosti s jednotlivými autentizačními metodami ale mohou ovlivnit vnímání těchto nebo jiných metod.



Graf 2: Zkušenosti s ověřením totožnosti pro přihlášení do online bankovnictví.

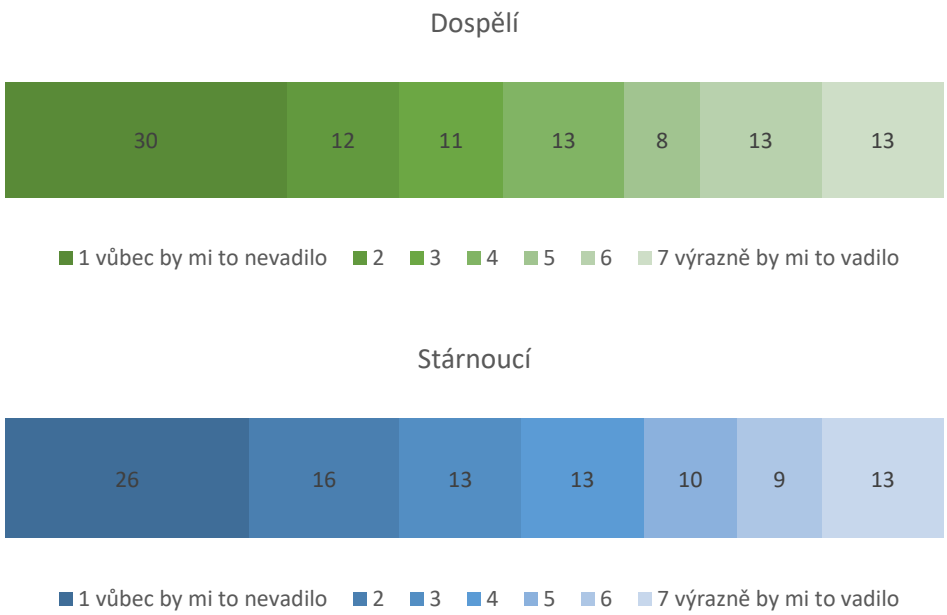
Při potvrzení plateb v online bankovnictví mělo nejvíce respondentů-uživatelů online bankovnictví zkušenost s SMS kódem, a to podobnou v obou populacích (95 % dospělých, 96 % stárnoucích), a následně PINem (50 % dospělých, 39 % stárnoucích) a heslem (51 % dospělých, 36 % stárnoucích), kde můžeme vidět rozdíly mezi dospělými a stárnoucími (viz Graf 3). Rozdíly mezi populacemi můžeme pozorovat také v případě otisku prstu, se kterým mělo zkušenost více dospělých osob (26 % dospělých, 11 % stárnoucích). S většinou způsobů potvrzení plateb v online bankovnictví měli dospělí osobní zkušenost častěji než stárnoucí.



Graf 3: Zkušenosti s potvrzováním plateb v online bankovnictví.

S placením online, např. kartou přes internet nebo převodem peněz v online bankovnictví, měla zkušenost většina dotazovaných (95 % dospělých, 82 % stárnoucích). Největší část uživatelů online bankovnictví uvedla, že platí online několikrát měsíčně (43 % dospělých, 41 % stárnoucích). Několikrát týdně platí online 24 % dospělých a 25 % stárnoucích uživatelů, denně pouze 4 % dospělých a 2 % stárnoucích uživatelů. 28 % dospělých a 27 % stárnoucích uživatelů uvedlo, že platí online pouze jednou měsíčně či méně často.

S ohledem na bezpečnostní rizika SMS kódu pro potvrzování plateb v online bankovnictví (detaily viz zde) hodnotili respondenti hypotetickou situaci, kdy by byla tato autentizační metoda plošně nahrazena jinou, na škále od 1 – vůbec by mi to nevadilo po 7 – výrazně by mi to vadilo. Přibližně polovina dospělých (53 %) i stárnoucích respondentů (55 %) odpověděla, že by jim taková změna nevadila (hodnota 1, 2 nebo 3), jak znázorňuje Graf 4. Výrazně (hodnota 6 nebo 7) by taková změna vadila 26 % dospělým a 22 % stárnoucím osobám, spíše by to vadilo (hodnota 5) dalším 8 % dospělých a 10 % stárnoucím. Neutrální postoj (hodnota 4) zastává shodných 13 % dospělých i stárnoucích. Lze tedy říci, že těch, kterým by nahrazení zasílání SMS kódu jinou autentizační metodou vadilo, je méně než těch, kterým by tato změna nevadila. Tato otázka však nebrala v potaz, jakou konkrétní autentizační metodou by SMS kód byl nahrazen.



Graf 4: Hodnocení nahrazení SMS kódu jinou autentizační metodou.

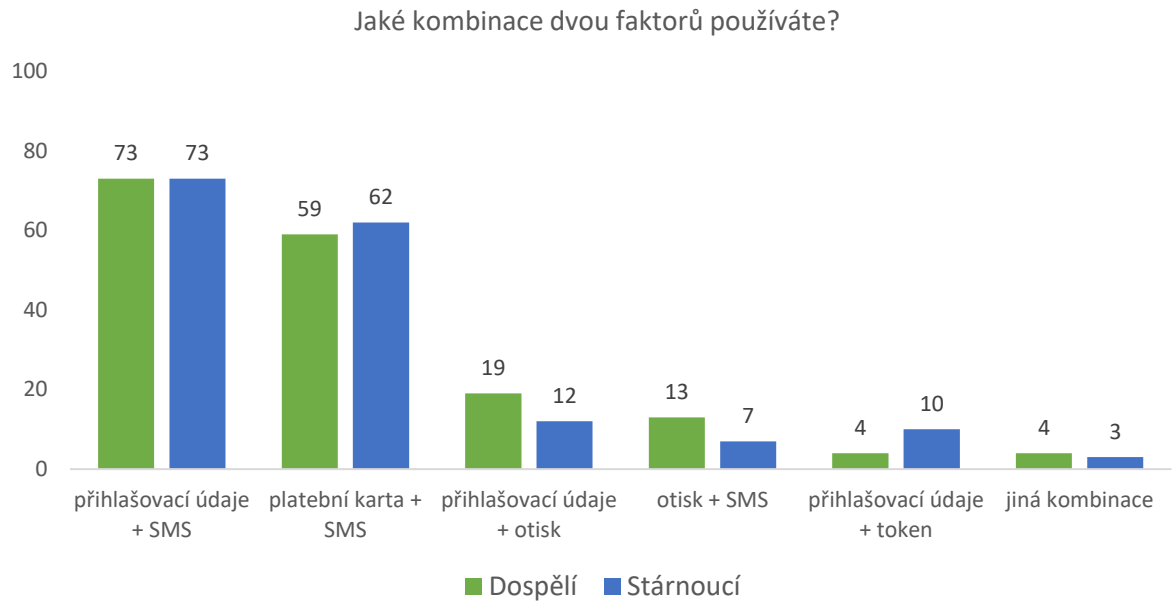
Dvoufaktorová autentizace

Další otázky se týkaly zkušeností s 2FA a ochotou ji používat pro různé scénáře.

Většina dotazovaných (84 % dospělých i stárnoucích) už dvoufaktorové ověření totožnosti v online službách někdy použila, takže koncept dvoufaktorové autentizace pro ně nebyl zcela neznámý. Konkrétně v online bankovnictví použití 2FA reportovalo 71 % dotazovaných dospělých a 69 % stárnoucích, při placení kartou online použití 2FA reportovalo shodných 59 % dospělých i stárnoucích respondentů. Přestože 2FA byla respondentům v rámci dotazníku vysvětlena, otázkou je, zda si byli všichni uživatelé vědomi toho, že 2FA např. pro potřeby online bankovnictví možná již používají.

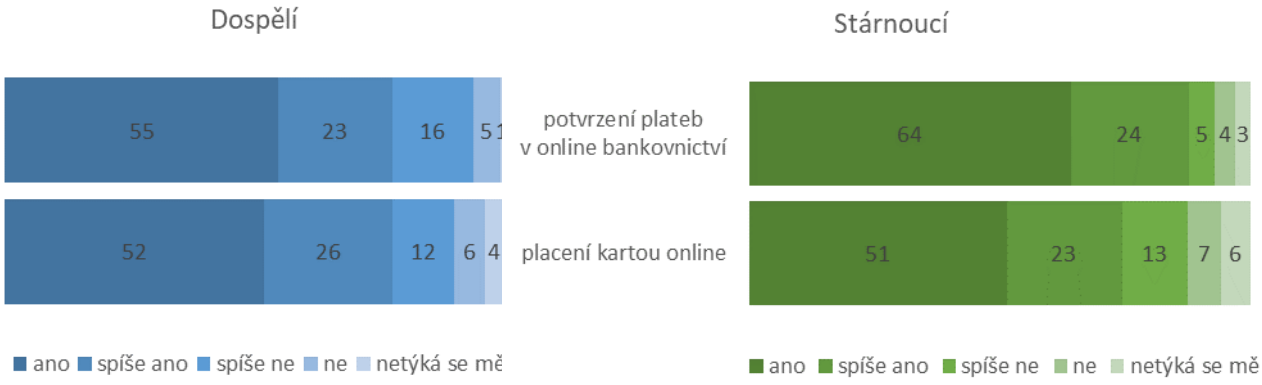
Dospělí uživatelé uvedli, že používají dvoufaktorovu autentizaci nejčastěji několikrát měsíčně (32 %) nebo několikrát týdně (29 %). Dále 11 % dospělých používá nějakou formu 2FA denně, zbytek (27 %) pak jednou či dvakrát měsíčně nebo méně často. Podobně je tomu u stárnoucí populace. Několikrát měsíčně 2FA používá 38 % stárnoucích, několikrát týdně 28 %. Denně používá nějakou formu 2FA 8 % stárnoucích. Dalších 25 % pak uvedlo, že 2FA používá jednou či dvakrát měsíčně nebo méně často.

Nejčastěji používanou kombinací faktorů jak u dospělých, tak u stárnoucích osob, které 2FA používají, byly přihlašovací údaje a potvrzovací SMS kód (73 % dospělých i stárnoucích), dále údaje z platební karty a potvrzovací SMS kód (59 % dospělých, 62 % stárnoucích). Výrazně méně často respondenti uváděli dvoufaktorové kombinace využívající otisk prstu či token, jak lze vidět v Grafu 5. Potvrzovací SMS kód v kombinaci s další metodou (přihlašovacími údaji nebo údaji z platební karty) tedy stále patří k nejrozšířenějším autentizačním metodám, které používají obě dotazované populace.



Graf 5: Četnost používání vybraných dvoufaktorových kombinací.

Následně byli respondenti dotázáni, zda by chtěli používat dvoufaktorovou autentizaci pro placení kartou online a pro potvrzování plateb v online bankovnictví (viz Graf 6). Shodných 78 % dospělých uvedlo, že by chtěli používat 2FA pro placení kartou online a pro potvrzování plateb v online bankovnictví. Stejně tak většina stárnoucích (74 %) by chtěla používat tento způsob ověření pro placení kartou online, a ještě více (88 %) pro online bankovnictví. Tato procenta jsou vyšší, než je podíl respondentů, kteří již 2FA v rámci placení kartou online nebo online bankovnictví použili (viz výše). Tyto odpovědi proto indikují obecně kladný postoj k 2FA pro finanční transakce napříč věkovými skupinami a zájem tento druh vyššího zabezpečení používat, a to i ze strany uživatelů, kteří s 2FA pro finanční služby neměli dosavadní zkušenost. Dotazovaní uživatelé si tedy zřejmě uvědomují důležitost ochrany svých finančních aktiv.

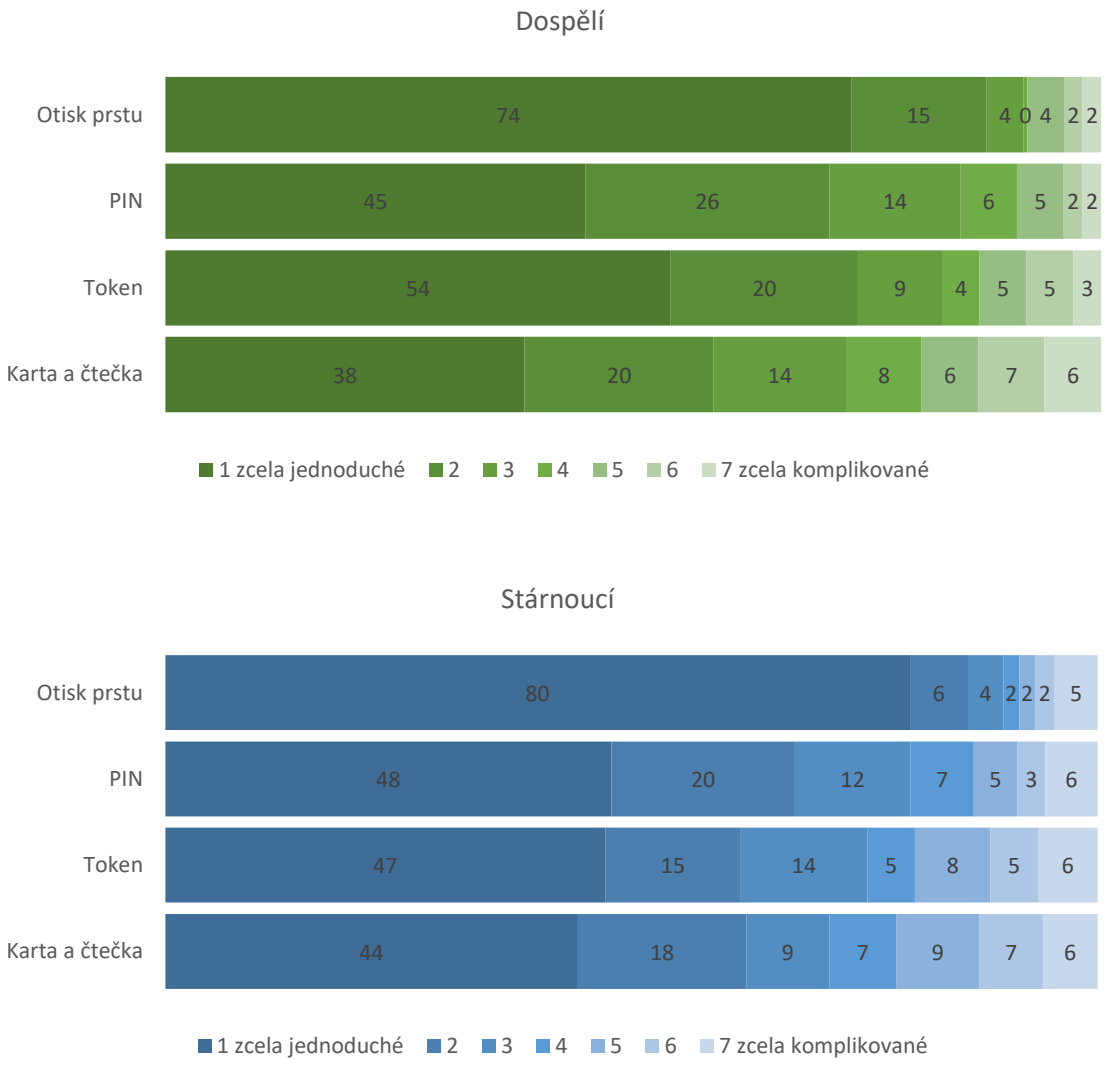


Graf 6: Ochota používat 2FA pro potvrzení plateb v online bankovnictví a placení kartou online.

Hodnocení testovaných autentizačních metod

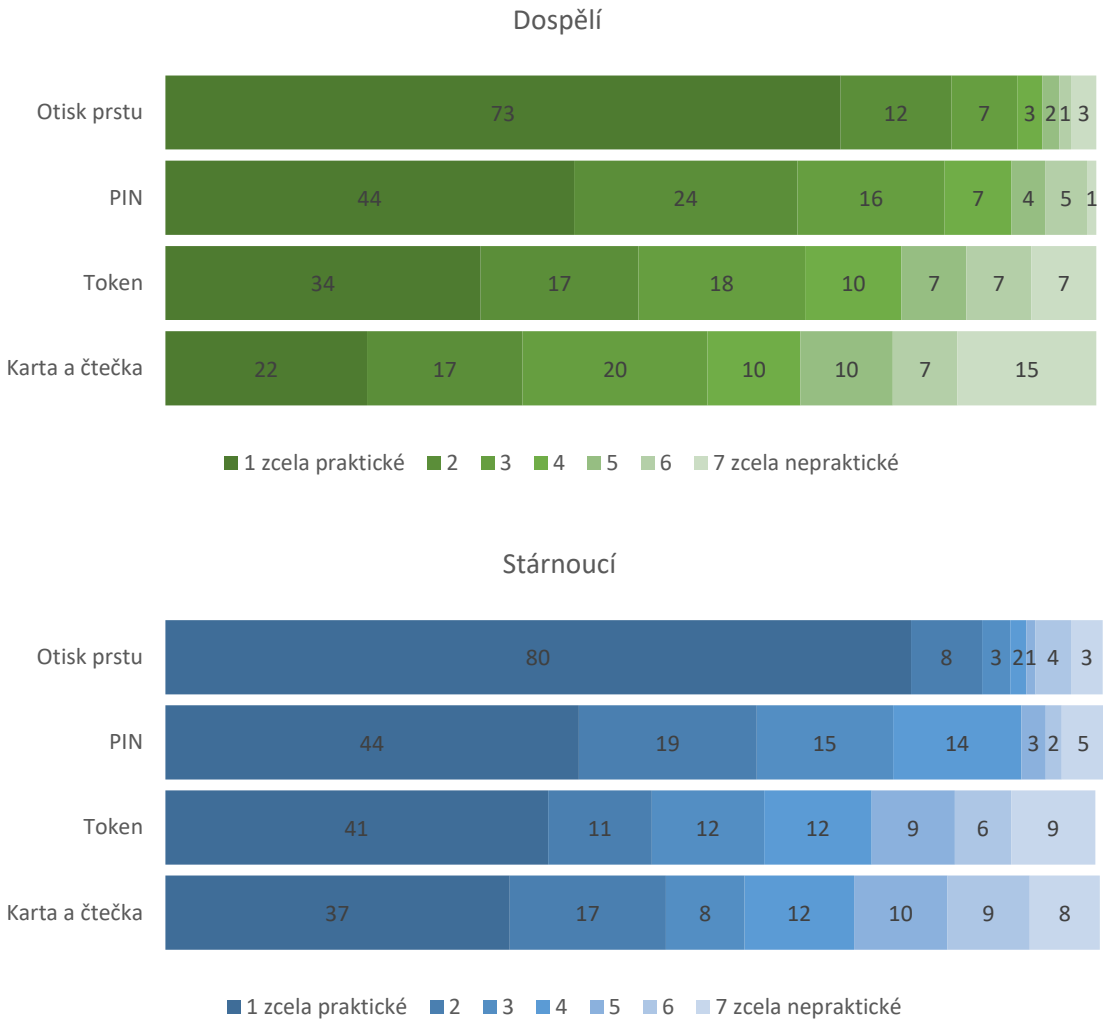
Respondenti dále posuzovali autentizační metody, které si vyzkoušeli při plnění úkolů na chytrém telefonu. Hodnotili, jak jsou *jednoduché na používání*, *praktické* a *bezpečné*.

Ohodnocení *jednoduchosti na používání* jednotlivých metod je zobrazeno na Grafu 7. Jako nejjednodušší na používání byl hodnocen otisk prstu. Pro většinu respondentů v obou populacích byl otisk prstu *zcela jednoduchý* na používání (74 % dospělých, 80 % stárnoucích). Pro více jak polovinu dospělé populace (54 %) byl i token *zcela jednoduchý* na používání, mezi stárnoucími hodnotilo token jako *zcela jednoduchý* 47 % respondentů. PIN byl v obou populacích hodnocen jako podobně jednoduchý jako token. Jako nejméně jednoduché na používání bylo oběma populacemi hodnocené vložení platební karty do čtečky. Jako *zcela jednoduché* jej hodnotilo 38 % stárnoucích a 44 % dospělých. Na druhé straně spektra hodnocení ho jako spíše či *zcela komplikované* vnímalo 19 % dospělých a 22 % stárnoucích.



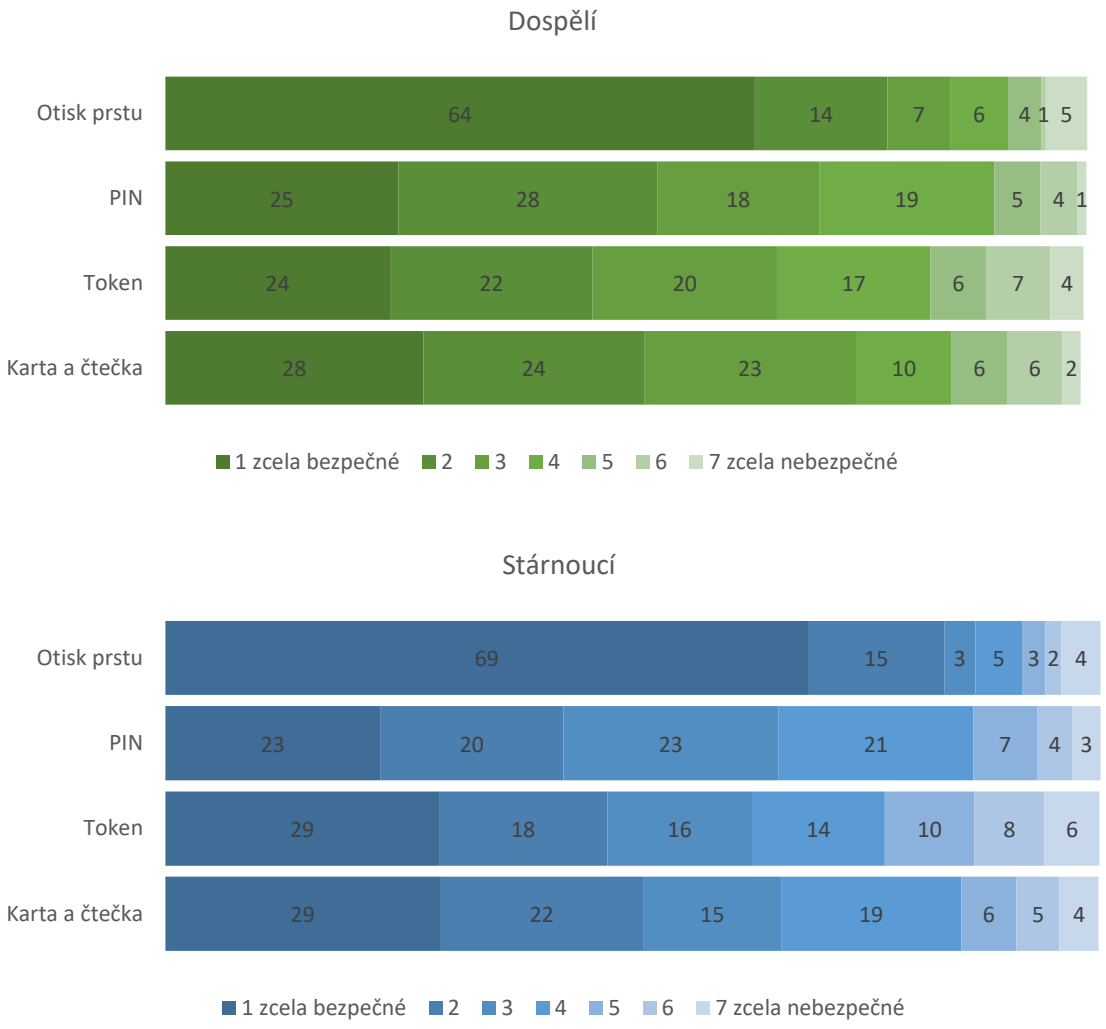
Graf 7: Hodnocení jednoduchosti používání testovaných metod.

Graf 8 zobrazuje hodnocení jednotlivých metod s ohledem na jejich vnímanou *praktičnost*. I z tohoto srovnání vyšel otisk prstu jako nejlépe hodnocená metoda. Jako *zcela praktický* ho vnímala většina obou zkoumaných populací (73 % dospělých, 80 % stárnoucích). PIN hodnotilo shodně 44 % obou populací jako *zcela praktický* a dalších 40 % dospělých, respektive 34 % stárnoucích, jako spíše praktický (hodnota 2 nebo 3). Přestože větší část stárnoucích hodnotila vložení platební karty do čtečky jako *zcela praktické* (37 % oproti 22 % dospělých), v součtu s hodnocením spíše praktické vnímalo vložení platební karty do čtečky pozitivně 59 % dospělých a 62 % stárnoucích. Více dospělých však čtečku hodnotilo jako *zcela nepraktickou* (15 % oproti 8 % stárnoucích). Podobně v případě tokenu ho hodnotilo jako *zcela praktický* více stárnoucích (41 % oproti 34 % dospělých), v součtu s hodnocením spíše praktické vnímalo token stran praktičnosti kladně 69 % dospělých a 64 % stárnoucích.



Graf 8: Hodnocení praktičnosti testovaných metod.

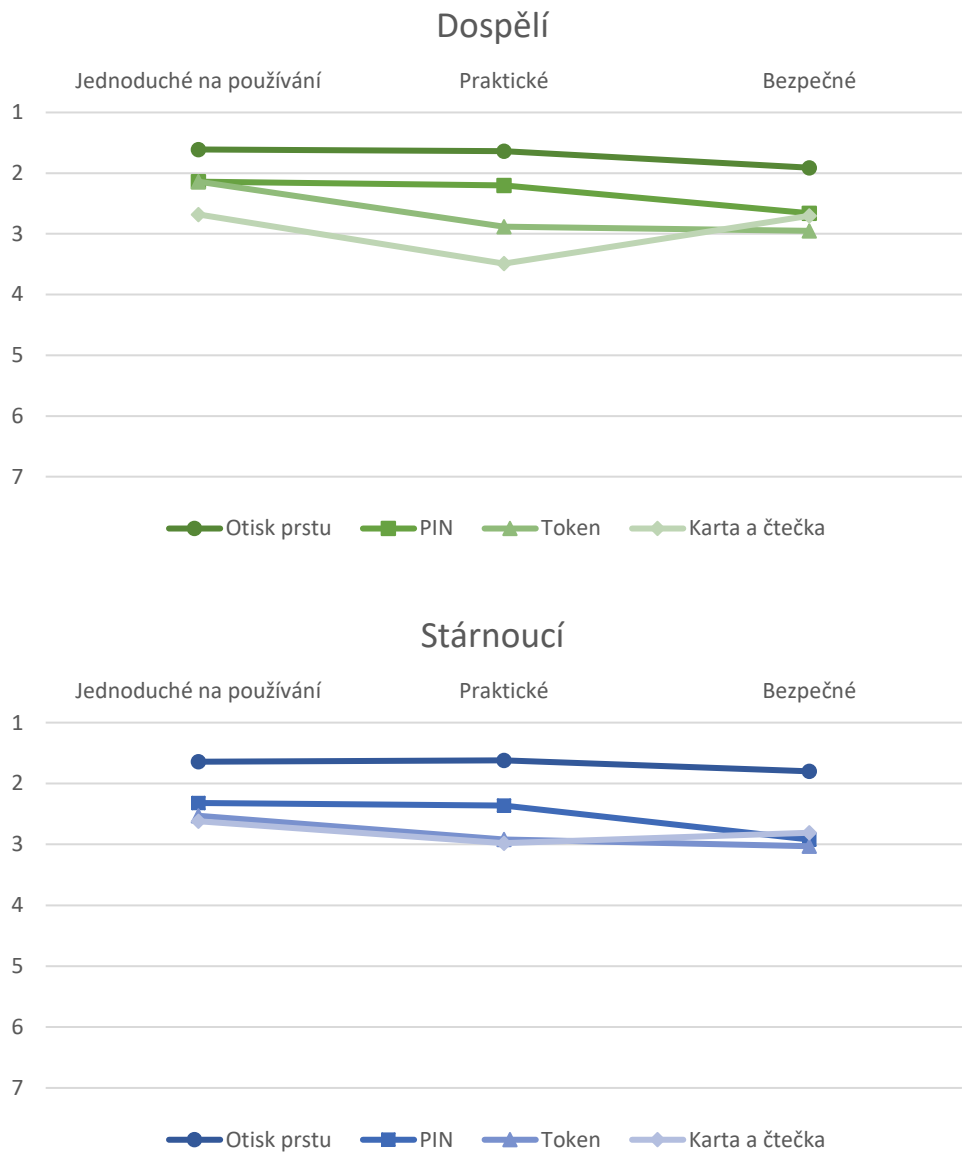
Poslední hodnocení se týkalo vnímané *bezpečnosti* jednotlivých metod, jak znázorňuje Graf 9. Otisk prstu byl opět hodnocen oběma populacemi jako nejvíce bezpečný. Jako *zcela bezpečný* ho hodnotilo 64 % dospělých a 69 % stárnoucích, dalších 21 % dospělých a 18 % stárnoucích ho hodnotilo jako spíše bezpečný (hodnota 2 nebo 3). Stárnoucí populace vnímala zbylé tři metody stran bezpečnosti podobně. o něco méně stárnoucích respondentů hodnotilo PIN jako *zcela bezpečný* (23 % oproti shodným 29 % u tokenu a vložení karty do čtečky), v součtu s hodnocením spíše bezpečné však metody hodnotilo jako bezpečné 66 % stárnoucích v případě PINu, 63 % v případě tokenu a 66 % v případě čtečky. Dospělá populace vnímala vložení platební karty do čtečky a použití PINu jako bezpečnější než token. Jako *zcela bezpečnou* hodnotilo čtečku 28 % dospělých, PIN 25 % a token 24 %. V součtu s hodnocením spíše bezpečné vnímalo čtečku kladně 75 % dospělých, PIN 71 %, token 66 %. V případě tokenu byl navíc v obou populacích největší podíl respondentů, kteří tuto metodu hodnotili jako spíše nebo *zcela nebezpečnou* (17 % dospělých, 24 % stárnoucích).



Graf 9: Hodnocení bezpečnosti testovaných metod.

Graf 10 ukazuje průměrná hodnocení jednotlivých metod na škále od 1 (nejlepší) do 7 (nejhorší). V celkovém hodnocení tedy obě populace vnímaly jednotlivé metody pozitivně ve všech třech zkoumaných oblastech. Otisk prstu byl vnímán jako nejjednodušší, nejpraktičtější a zároveň nejvíce bezpečná metoda oběma populacemi, a to navzdory tomu, že jeho reálná bezpečnost není příliš vysoká (podrobnosti zde). I ostatní metody však byly obecně hodnoceny pozitivně.

Autentizační metody založené na vlastnictví předmětu (konkrétně token a karta + čtečka) byly hodnoceny stárnoucí populací velmi podobně ve všech třech oblastech. Naproti tomu dospělá populace vnímala vložení karty do čtečky jako méně jednoduché a méně praktické než použití tokenu. Použití PINu bylo oběma populacemi hodnoceno podobně, a sice méně jednoduché, praktické a bezpečné než otisk prstu, ale praktičtější a podobně bezpečné jako token a vložení karty do čtečky.



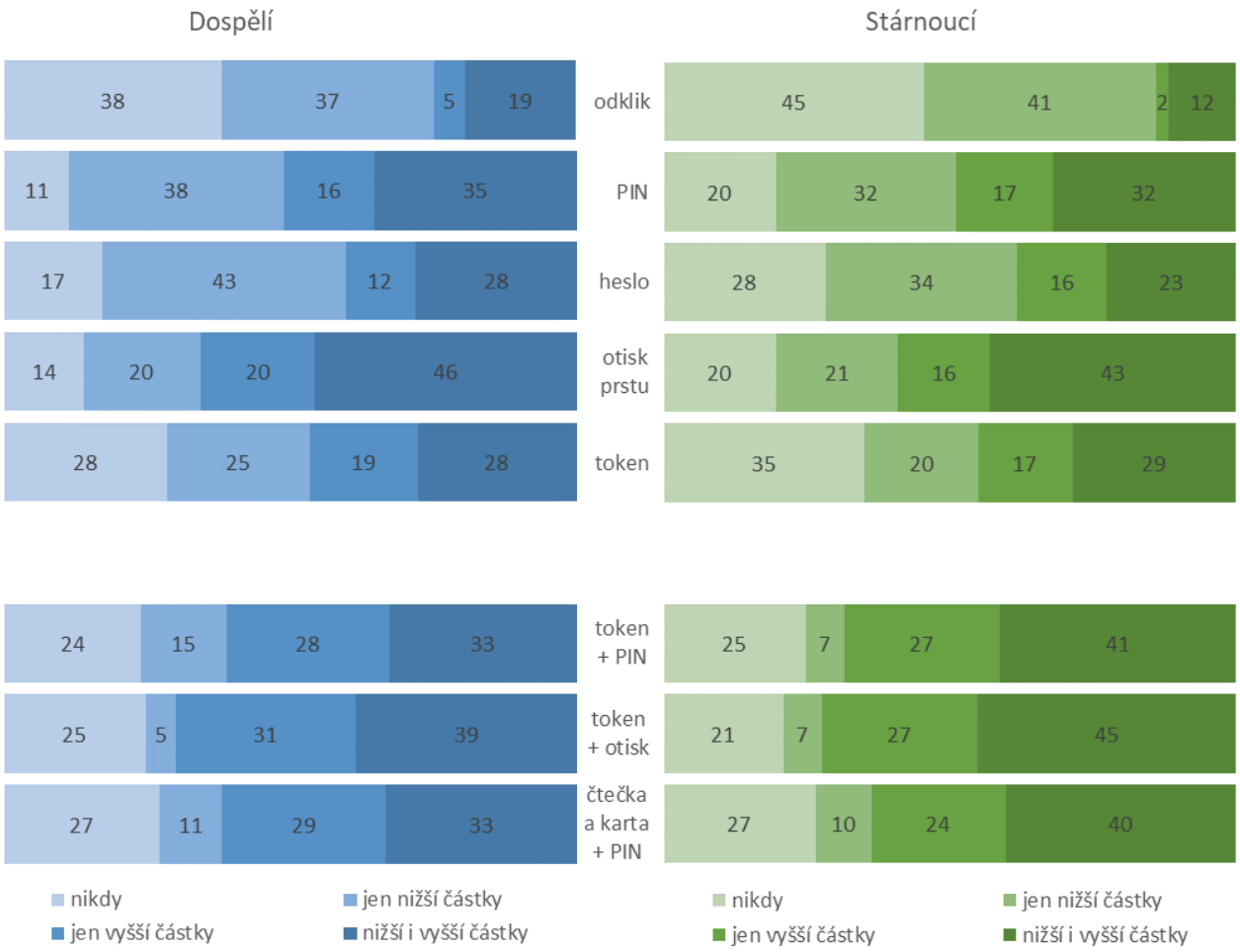
Graf 10: Srovnání průměrného hodnocení jednoduchosti používání, praktičnosti a bezpečnosti jednotlivých metod.

Preference autentizačních metod pro potvrzování plateb

Nakonec jsme se respondentů ptali, pro jaké částky při potvrzování transakcí po přihlášení do online bankovnictví by chtěli používat jednotlivé autentizační metody. Kromě testovaných metod zde byly přidány také další, netestované kombinace, které uživatelé znali ze svého chytrého telefonu nebo si je dokázali představit na základě zkušenosti získané při testování. Na výběr měli z následujících možností: nikdy bych danou metodu nechtěl(a) používat, pouze pro nižší částky, pouze pro vyšší částky, pro nižší i vyšší částky (tedy pro potvrzování všech finančních transakcí). Hranice mezi nižší a vyšší částkou nebyla explicitně stanovena a jednalo se tedy o subjektivní vnímání této hranice respondenty. Kompletní výsledky popisuje Graf 11.

Použití nějaké autentizační metody pro potvrzování plateb v online bankovnictví je žádoucí, protože pouhé odkliknutí platby (tedy bez použití další autentizační metody) bylo nejvíce odmítanou formou potvrzení plateb. 38 % dospělých a 45 % stárnoucích uživatelů by nikdy nechtělo platbu pouze odkliknout. Na druhou stranu zde byli i lidé, kterým by pouhé odkliknutí bylo dostatečné, chtěli by ho však používat spíše pro nižší částky (37 % dospělých, 41 % stárnoucích). Samotný token bez dalšího faktoru by nechtělo nikdy používat 28 % dospělých, 35 % stárnoucích. Naopak mezi jednofaktorové metody, které by chtěli dotazovaní používat pro potvrzování jakkoli vysoké transakce v online bankovnictví, patřil otisk prstu (46 % dospělých, 43 % stárnoucích), což je v souladu s hodnocením této metody jakožto použitelné, praktické a zároveň bezpečné. Druhou nejvíce preferovanou 1FA metodou pro jakékoliv částky byl číselný PIN (35 % dospělých, 32 % stárnoucích), který měl hned po otisku prstu nejvyšší průměrné hodnocení v jednoduchosti a praktičnosti.

Hodnocení dvoufaktorových metod bylo vyrovnanější než hodnocení metod jednofaktorových. V případě všech 2FA kombinací lze obecně říci, že existovala přibližně pětina osob (21-27 %), která by danou kombinaci nikdy nechtěla používat. To je však patrně dáno preferencí jiné kombinace metod. Na druhou stranu, nadpoloviční většině respondentů (v součtu 51-72 %) dávalo smysl jednotlivé kombinace metod používat pro potvrzení plateb o vyšších částkách, konkrétně by dané 2FA kombinace chtělo pro všechny platby využívat 33-45 % respondentů, pouze pro vyšší platby pak 24-31 %. Dále bylo patrné, že použití 2FA pouze pro nižší částky nedává respondentům smysl a tyto preference jsou v menšině (5-15 %). V populaci dospělých i stárnoucích byla mírně preferovaná kombinace využívající otisku prstu, tedy otisku prstu + token. Pro potvrzování všech plateb by tuto kombinaci chtělo využívat 39 % dospělých a 45 % stárnoucích, pouze pro platby o vysokých částkách pak 31 % dospělých a 27 % stárnoucích. Zbylé dvě 2FA kombinace, PIN + token a karta ve čtečce + PIN ke kartě byly v rámci jednotlivých populací hodnoceny velmi podobně.



Graf 11: Preference autentizačních metod pro potvrzování plateb různé výše.

Literatura

Doležal, P., Dařbujanová, A., & Knapová, L. (2019). Jak uživatelé přemýšlejí o bezpečnosti v kontextu mobilního bankovnictví. *Data Security Management, 2019*(2), 11-15. Dostupné na: https://tate.cz/archiv-2019/893-dsm-2019-2

Mayes, K. & Markantonakis, K. (2017). *Smart cards, tokens, security and applications.* Cham, Switzerland: Springer.

Paul, G., & Irvine, J. (2016). IEDs on the Road to Fingerprint Authentication: Biometrics have vulnerabilities that PINs and passwords don't. *IEEE Consumer Electronics Magazine, 5*(2), 79–86.

Přílohy

Příloha 1: Dopis od banky popisující postup aktivace aplikace IDport s použitím tokenu

YourBank.

Pokyny pro aktivaci

Vážená paní, vážený pane,

děkujeme za Váš zájem využívat naši novou mobilní aplikaci IDport, která slouží k ověřování Vaší totožnosti při kontaktu s Vaší bankou. Níže najdete instrukce, jak aplikaci aktivovat.

Pro aktivaci aplikace využíváme kombinaci dvou údajů:

A **Klientské jméno a aktivační kód / QR kód**

B **NFC token**

Aktivace je tak bezpečnější. Využití dvou údajů zajišťuje, že aplikaci aktivujete přímo Vy a ne někdo, kdo se k jednomu z údajů dostal náhodou.

Věříme, že s naší službou budete spokojeni.

Vaše YourBank

1. Spusťte aplikaci IDport

2A. Pomocí aplikace naskenujte QR kód	2B. Zadejte přihlašovací údaje
A1	KLIENTSKÉ JMÉNO: uzivatel@test.cz AKTIVAČNÍ KÓD 29607 A2

YourBank.

Pokyny pro aktivaci

3. Přiložte token na NFC čtečku	4. Zvolte si osobní PIN
	
	5. Zvažte použití otisku prstů
	

PODĚKOVÁNÍ

Na tomto místě bychom chtěli poděkovat všem, kdo nám pomohli s realizací tohoto výzkumu. Předně děkujeme všem respondentům, kteří se zúčastnili našeho testování. Dále patří velké poděkování všem tazatelům a pomocníkům se sběrem a zpracováním dat.

Technická zpráva byla podpořená Technologickou agenturou České republiky v rámci projektu TL01000207 Inovace a adaptace autentizačních technologií pro bezpečné digitální prostředí.

Kontakt

prof. PhDr. **David Šmahel**, Ph.D.

Institut výzkumu dětí, mládeže a rodiny, Fakulta sociálních studií
Katedra strojového učení a zpracování dat, Fakulta informatiky
Masarykova univerzita, Brno

E-mail: smahel@fss.muni.cz
Telefon: +420 604 234 898

Mgr. **Ondřej Gabrhelík**

AHEAD iTec, s.r.o.
Team Leader

E-mail: ondrej.gabrhelik@ahead-itec.com
Telefon: +420 731 196 750

Interdisciplinary Research Team on Internet and Society

http://www.irtis.muni.cz/

Center for Research on Cryptography and Security

https://crocs.fi.muni.cz/

AHEAD iTec, s.r.o.

https://idport.cz/tacr/

MUNI Interdisciplinary Research Team on Internet and Society

CROCS