فصلنامه مطالعات نوین بانکی

ISSN: 2645-5420 شماره مجوز: 83289

بررسی تأثیر الزامات فنی و کاربردی رمزهای پویا در میزان رضایتمندی مشتریان بانکی

(تاریخ دریافت۱۳۹۸/۰۵/۰۲ ، تاریخ تصویب ۱۳۹۸/۱۱/۲۰)

علی سلیمانی[1]

عضو هیئت‌علمی موسسه آموزش عالی الکترونیکی ایرانیان

فاطمه عرب گل

کارشناس ارشد شبکه و امنیت شرکت بهسازان ملت

چکیده

یکی از روش‌های حفظ امنیت حساب بانکی و جلوگیری از حدس رمز دوم ضعیف، استفاده از رمزهای یکبارمصرف می‌باشد. رمز یکبارمصرف برای ایمن‌سازی دسترسی کاربران به سیستم‌های الکترونیکی است که در آن از الگوریتم‌های رمزنگاری و تابع چکیده‌سازی برای تولید رمز تصادفی یکبارمصرف با طول عمر محدود استفاده می‌شود. اجرای طرح الزام استفاده از رمز دوم پویا برای تراکنش‌های بدون کارت، تعداد جرائم فیشینگ را به صفر رسانده و ضریب امنیتی بالایی برای مشتریان فراهم می‌آورد. در این مقاله ضمن تشریح فرآیند احراز هویت توسط رمز یکبارمصرف و انطباق آن با الزامات رمزپویا ابلاغ شده توسط بانک مرکزی، مقایسه‌ای بر روی روش‌های فعال‌سازی و اپلیکیشن‌های تولید رمز یکبارمصرف در بانک‌های مختلف کشور انجام شده است. در بخش دیگری از این مقاله نیز نتایج یک نظرسنجی عمومی در مورد مقبولیت رمز یکبارمصرف از مشتریان بانک‌های مختلف تحلیل و بررسی شده و در پایان نیز پیشنهاداتی در راستای افزایش رضایتمندی عمومی ارائه‌شده است.

واژگان کلیدی: رمز یکبارمصرف، رمز پویا، بانکداری الکترونیک، مهندسی اجتماعی، بانک

[1] نویسنده مسئول

مقدمه

بانکداری الکترونیکی شیوه‌ای از بانکداری شامل خدمات مختلف بانکی است که با استفاده از آن، مشتری در تمامی ساعات شبانه‌روز و بدون حضور فیزیکی در شعب بانک، می‌تواند از طریق درگاه‌های مختلف نظیر پایانه فروش، درگاه‌های اینترنتی، خودپرداز، تلفن ثابت و تلفن همراه با استفاده از سرویس‌های امن الکترونیکی از قبیل همراه بانک، تلفن‌بانک، اینترنت بانک و کدهای دستوری که بانک در اختیار او قرار می‌دهد، از خدمات بانکی استفاده نماید. با توجه به گستردگی تراکنش‌های بانکی و انجام حداکثری تراکنش‌ها در بستر اینترنت و بانکداری الکترونیکی که منجر به افزایش مبادلات در این حوزه شده است، لزوم به‌کارگیری شیوه‌های مدرن در جهت افزایش امنیت این نوع تراکنش‌ها ضروری به نظر می‌رسد. رمز یکبارمصرف یا رمز پویا یک جایگزین برای رمز دوم می‌باشد که برای امن سازی تراکنش‌های بانکی ارائه‌شده و در آن از قابلیت‌های رمزنگاری برای تولید رمز تصادفی یکبارمصرف با عمرمحدود استفاده می‌شود. مهم‌ترین علتی که باعث شده تا این تکنولوژی به فرآیند سیستم بانکی وارد شود آن است که برنامه نویسان و مهندسان شبکه، می‌توانند امنیت در حوزه سرویس‌دهنده (مبدأ خدمت) را افزایش دهند اما در سمت کلاینت یا سرویس‌گیرنده (مقصد خدمت) توان افزایش امنیت بسیار محدود است، چراکه بسیاری از خدمات بانکی بر بستر مرورگرها انجام می‌شود و یکی از رایج‌ترین ضعف‌های سمت سرویس‌گیرنده که قربانیان زیادی را نیز داشته است، سرقت رمز عبور و رمز دوم کارت مشتریان است تا جایی که بیش از ۶۰ درصد پرونده‌های پلیس فتا مربوط به سرقت اطلاعات کارت‌بانکی و برداشت غیرمجاز از حساب مشتریان است و در سال جاری حدود ۲۳ هزار پرونده در این خصوص تشکیل‌شده است[۱] . مهاجمان و مجرمان سایبری به‌راحتی و با

استفاده از نرم‌افزارها و سخت‌افزارهای کی‌لاگر[1] یا طراحی وب‌سایت‌های جعلی و فریب کاربران از طریق حملات مهندسی اجتماعی، قابلیت آن را دارد تا اطلاعات و پسوردهای بانکی کاربران را سرقت کنند. تأیید اعتبار یا احراز هویت چندعاملی، مکانیزمی است که می‌تواند حتی در صورت سرقت اطلاعات حساب کاربران و رمز دوم کارت، برداشت غیرمجاز را بسیار کاهش داده و به تقریباً به صفر برساند، چراکه گذرواژه قربانی یا رمز دوم کارت برای انجام تراکنش بانکی دیگر کافی نخواهد بود. بااین‌حال، بسیاری از رویکردهای احراز هویت چندعاملی در برابر فیشینگ مرورگر و حملات مرد میانی آسیب‌پذیر هستند[۲] بهترین راهکار مقابله با مجرمان سایبری و کی‌لاگرها استفاده از رمزهای یکبارمصرف است چراکه رمز پویا صرفاً یکبار و برای مدت‌زمان محدودی قابل‌استفاده بوده و مجدداً نمی‌توان از این گذرواژه استفاده کرد و انجام تراکنش بانکی نیازمند رمز عبور جدیدی است که تکرار حملات را غیرممکن می‌سازد.

بخش اول: پیشینه استفاده از رمز پویا

حملات به بانکداری اینترنتی اولین بار در سال ۲۰۰۱ پس از حملات ۱۱سپتامبر از طریق فیشینگ[2] ایمیل بر روی سامانه‌های مالی مورد هدف قرار گرفت. از سال ۲۰۰۴ به بعد، این صنعت شاهد افزایش چشمگیر حملات علیه مؤسسات مالی بوده است. به‌موازات گستردگی در انواع حملات، پیچیدگی حملات نیز مشاهده‌شده است که لزوم آشنایی کارشناسان امنیتی بانکداری با تکنیک‌ها و اصلاحات متنوع و پیچیده این حملات بسیار قابل‌ملاحظه می‌باشد که از بین این حملات می‌توان به حملات فیشینگ، فارمینگ[3]، فیشینگ هدف‌دار[4]، سرقت نشست[5]، مرد میانی[1]، مردی در

[1] Keylogger
[2] Phishing
[3] Pharming
[4] Spear Phishing
[5] Session Hijacking

مرورگر[۲]، تروجان‌ها[۳]، راک فیش[۴] و غیره اشاره نمود. علیرغم تنوع درروش های حمله، اکثر این حملات برای به دست آوردن یک هدف اصلی انجام می‌گردد و آن شامل دستیابی به اطلاعات محرمانه کاربر مانند نام های کاربری، کلمه عبور، شماره کارت‌های اعتباری و شماره‌های تأمین اجتماعی می‌باشد که تمامی این موارد مدارک معتبر و استاتیک هستند که تغییر نمی‌کنند و مشکل اینجاست که پس از به دست آوردن آن‌ها توسط مهاجم، قادر به جعل اطلاعات مشتری برای ارتکاب تقلب مورداستفاده قرار می‌گیرند[۳] . استفاده از احراز هویت دوعاملی برای مقابله با این حملات مؤثر واقع شد که به‌عنوان بخشی از استراتژی لایه‌های امنیتی محسوب می‌گردد. به‌طورکلی کلیه مکانیسم‌های سیستم‌های شناسایی تائید اعتبار و احراز هویت را دریکی از سه دسته زیر قرار می‌گیرند:

- چیزی که شما می‌دانید مانند رمزهای عبور
- چیزی که شما دارید مانند کارت‌های هوشمند اعتباری و بانکی و یا انواع Tokenها
- چیزی که شما هستید مانند اثرانگشت، تصویر چهره، ساختار شبکیه و عنبیه چشم

رمزهای OTP یک‌شکل آسان و قابل اعتماد از احراز هویت دومرحله‌ای است و برای اضافه کردن لایه دوم تأیید اعتبار استفاده می‌شود. کاربر ملزم به واردکردن رمز یکبارمصرف خود علاوه بر نام کاربری و رمز عبور می‌باشد که این امر، خطر تقلب را به شدت کاهش می‌دهد. در بسیاری از کشورهای جهان رمز دوم یکبارمصرف به‌منظور جلوگیری از حملات و کلاه‌برداری‌های

---

[1] Man-In-The-Middle
[2] Man-In-The-Browser
[3] Trojan
[4] Rock Phish

اینترنتی استفاده می‌شود. رمز پویا درواقع نوعی احراز هویت چندعاملی[1] است که در بسیاری از سرویس‌ها ازجمله پست الکترونیکی و پیام‌رسان‌ها استفاده می‌شود. به‌کارگیری این رمز بسیاری از معایب رمز ایستا را برطرف می‌کند. بنا به ادعای مایکروسافت، استفاده از احراز هویت چندعاملی، کاربران را در برابر ۹۹/۹ درصد حملات مصون می‌کند، گوگل نیز ادعا می‌کند با استفاده از تأیید چندمرحله‌ای، می‌توان جلوی ۹۹ درصد حملات فیشینگ[2] را گرفت[۴] ازاین‌رو برای مقابله با تهدیدات امنیتی بانکداری الکترونیک که می‌تواند خسارات مالی هنگفتی برای مشتریان بانک‌ها در پی داشته باشد، ارتقای سطح آگاهی عمومی و لزوم پیاده‌سازی راهکاری با ضریب امنیت بالا حائز اهمیت است. از سال ۲۰۰۵، شورای بررسی آزمون‌های موسسه مالی فدرال ایالات‌متحده[3] دستورالعمل‌هایی برای مؤسسات مالی ارائه داد که موظف به بررسی ارزیابی‌های مبتنی بر ریسک شدند و استفاده از برنامه‌هایی را توصیه می‌کنند که آگاهی مشتری را افزایش داده و اقدامات امنیتی را برای تأیید صحت اعتبار مشتریان از راه دور برای دسترسی به خدمات مالی آنلاین فراهم می‌کند [۵]. بنابراین تأیید پرداخت با استفاده از رمزهای یکبارمصرف از روش‌های مرسوم بانک‌های اغلب کشورهای جهان است. بدین معنی که مشتریان بانک‌ها برای خریدهای اینترنتی و واریز وجه بیشتر مواقع ملزم به دریافت رمز یکبارمصرف به‌مدت زمان محدود و از طریق پیامک یا برنامه‌های نرم‌افزاری هستند. بیشتر بانک‌های بزرگ و معتبر جهان مانند **Bankof America** خدمات ارسال رمز دوم پویا را از طریق پیامک به مشتریان خود ارائه می‌دهند. البته سیاست اجبار به استفاده از این روش‌ها هنگام خرید آنلاین در بین بانک‌ها متفاوت است. برای مثال **Bank of**

[1] MFA (Multi-Factor Authentication)

[2] Phishing

[3] Federal Financial Institutions Examination Council's ((FFIEC's)

Americaاستفاده از رمز یکبارمصرف (که آن را **SafePass** می‌نامد) را از سال ۲۰۱۸ از حالت اجباری خارج کرده است.

در جدول شماره ۱ برخی از بانک‌هایی از کشورهای جهان که از شیوه‌های مختلف رمز یکبارمصرف استفاده می‌کنند آورده شده است [۶].

جدول شماره ۱ – نمونه بانک‌های استفاده‌کننده از رمز پویا در سایر کشورها

نام بانک	توکن نرم‌افزاری	توکن سخت‌افزاری	پیامک	پست الکترونیک
Bank Central Asia (Indonesia)		✓		
(Czech Republic)Airbank	✓		✓	
Bank of China (Hong Kong)		✓		
Citi Bank (United Satate)		✓	✓	✓
Post Bank (Germany)	✓	✓		
(Croatia)Erste Bank Hrvatska	✓	✓		
Bank (Malaysia) May		✓	✓	

بخش دوم: الزامات فنی رمزهای پویا در تراکنش‌های مبتنی بر کارت

رمز یکبارمصرف یا OTP[1] یک روش بلااثر کردن سرقت رمز عبور می‌باشد که با استفاده از روش‌های رمزنگاری و توابع درهم‌سازی[2] تولیدشده و تنها برای یکبار ورود به سیستم معتبر است. مهم‌ترین مزیت استفاده از رمز یکبارمصرف این است که سرقت اطلاعات با دانستن رمز عبور غیرممکن می‌گردد. تکنولوژی **OTP** جهت انجام تراکنش‌های امن بانکی بر بستر اینترنت کاربرد

[1] One Time Password
[2] Hash Function

دارد و بر اساس برنامه کاربردی تلفن همراه یا ابزاری که توسط بانک به مشتری داده می‌شود، برای انجام هر تراکنش یک رمز تولید می‌شود که تنها یکبار اعتبار دارد. در این تکنولوژی رمز یکبارمصرف بر اساس الگوریتم تعریف‌شده در ابزار کاربر و در سرور مرتبط تولید می‌شود و دارای انواع مختلفی نظیر **TOTP**[1]، **HOTP**[2] می‌باشد. امنیت **OTP** به دلیل استفاده از توابع رمزنگاری و درهم‌سازی، بسیار بالا می‌باشد. بانک مرکزی جمهوری اسلامی ایران در سندی با عنوان «الزامات رمزهای پویا در تراکنش‌های مبتنی بر کارت» [۷] که در شهریور ۱۳۹۷ منتشرشده است به بیان حداقل الزاماتی پرداخته است که بانک‌ها و مؤسسات اعتباری باید در خصوص تولید و استفاده از رمز پویا مرتبط با کارت‌های بانکی رعایت کنند. در این بخش، ضمن بررسی الگوریتم‌های مورد تأیید بانک مرکزی، پارامترهای ورودی توابع تولید رمز پویا از دو منظر پیش‌فرض سند **RFC** و حداقل قابل قبول بانک مرکزی مورد بررسی قرار گرفته است.

بند اول: فرآیند احراز هویت با رمز یکبار مصرف

- **الگوریتم HOTP**

سازوکار این الگوریتم که در **RFC-۴۲۲۶** تشریح شده است [۸] مبتنی بر روش احراز هویت پیام **HMAC**[3]می‌باشد و رمز یکبارمصرف را طبق فرمول (۱) تولید می‌کند:

$$HOTP(K, C) = truncate(HMAC_H(K, C)) \quad (1)$$

که در آن، **truncate** تابعی است که مقدار **HMAC-SHA-۱** را به یک مقدار **HOTP** تبدیل می‌کند و پارامترهای آن عبارت‌اند از:

[1] Time-based One Time Password
[2] HMAC-based One Time Password
[3] Hash-based Message Authentication Codes

۱) تابع درهم‌ساز **H** (پیش‌فرض سند **RFC-۴۲۲۶** تابع **SHA-۱** می‌باشد اما به دلیل ضعف اثبات‌شده آن[۹] ، در سند الزامات رمزهای پویا در تراکنش‌های مبتنی بر کارت، استفاده از **SHA-۱** و **MD۵** توسط بانک مرکزی منع شده است.)

۲) کلید خصوصی و محرمانه **K** که بین مشتری و سرویس‌دهنده به اشتراک گذاشته می‌شود. این کلید برای هر مشتری متفاوت و منحصربه‌فرد است. (که طبق دستورالعمل بانک مرکزی، حداقل باید ۱۱۲ بایت باشد.)

۳) طول رمز یکبارمصرف **C** یا به‌عبارت‌دیگر، یک شمارنده است که باید بین تولیدکننده رمزیکبار مصرف (مشتری) و سامانه اعتبارسنجی (سرور) همگام باشد. (که حداقل ۶ و حداکثر ۱۰ رقم می‌تواند باشد. پیشنهاد سند **RFC-۴۲۲۶**، ۸ رقم و طبق دستورالعمل بانک مرکزی، حداقل طول رمز پویا باید ۷ رقم باشد.)

فرایند تولید و اعتبارسنجی رمزیکبارمصرف مبتنی بر الگوریتم **HOTP** را در سه مرحله می‌توان بیان کرد**[۱۰]** :

a. یک مقدار **HMAC-SHA-۱** تولید می‌شود:

$$HS = HMAC\text{-}SHA\text{-}1(K, C) \quad (3)$$

b. یک‌رشته ۴ بایتی تولید می‌شود:

$$Sbits = DT(HS) \quad (4)$$

DT returns a 31-bit string

c. مقدار **HOTP** محاسبه می‌شود:

Snum = StToNum (Sbits)

(5)

مقدار **S** به عددی در محدوده ۱-^{۳۱}۲...۰ تبدیل می‌شود:

Return D = Snum mod 10 ^ **Digit**

(6)

مقدار **D**، عددی در محدوده ۱-$^{\text{Digit}}$۱۰...۰ است و **Digit**، تعداد رقم‌های مقدار **HOTP** می‌باشد.

تابع **Truncate** مراحل ۲ و ۳ را جهت کاهش پویا اجرا کرده و تعداد ارقام را به پیمانه $^{\text{Digit}}$۱۰ کاهش می‌دهد. هدف از تکنیک کاهش با میزان انحراف پویا، استخراج یک کد باینری ۴ بایتی پویا از رشته ۲۰ بایتی **HMAC-SHA-۱** است. شبه کد تابع **DT** به شرح زیر است:

DT (String)
Let OffsetBits be the low-order 4 **bits of String**[19]
Offset = StToNum (OffsetBits)
Let P = String[OffSet]...String[OffSet+3]
Return the Last 31 **bits of P**
End (DT)

که در آن:

String=String[0]...**String**[19]

(8)

0 <= **OffSet** <= 15

(9)

علت حذف باارزش‌ترین بیت **P**، جلوگیری از سردرگمی در مورد محاسبات اعداد علامت‌دار و اعداد بدون علامت است. پردازنده‌های مختلف، این توابع را به‌صورت متفاوتی اجرا می‌کنند و

حذف بیت علامت، تمام ابهامات را برطرف می‌کند. خروجی این تابع منجر به یک با طول حداقل ۶ و حداکثر ۸ رقم خواهد شد.

- **الگوریتم TOTP**

سازوکار این الگوریتم که در **RFC-۶۲۳۸** تشریح شده است[۱۱] مبتنی بر الگوریتم **HOTP** و روش احراز هویت **OATH**[1] می‌باشد و رمز یکبارمصرف را طبق فرمول (۲) تولید می‌کند:

$$\text{TOTP value } (K) = \text{HOTP value } (K, C_T) \quad (10)$$

$$C_T = (\text{Timestamp curent} - T_0)/X \quad (11)$$

که پارامترهای آن عبارت‌اند از:

۱) شمارنده زمان C_T یک عدد صحیح بوده و بیانگر گام‌های زمانی بین مقدار اولیه شمارنده زمان **T**. و زمان جاری سیستم **Unix** می‌باشد (به‌طور مثال، تعداد ثانیه‌های سپری‌شده از نیمه‌شب ۱ ژانویه ۱۹۷۰)

۲) کلید خصوصی و محرمانه **K** (که طبق دستورالعمل بانک مرکزی، حداقل باید ۱۱۲ بایت باشد.)

۳) **X** بیانگر گام‌های زمانی برحسب ثانیه بوده مدت‌زمان اعتبار رمز (پیش‌فرض سند **RFC-۶۲۳۸**، ۳۰ ثانیه می‌باشد. در دستورالعمل بانک مرکزی، حداکثر طول عمر رمز پویا باید حداکثر ۶۰ ثانیه بوده و پس‌ازاین زمان، رمز تولیدشده منقضی و غیرقابل استفاده شود.)

بانک مرکزی، علاوه بر الزامات ذکرشده در تشریح الگوریتم‌های فوق، ملاحظات دیگری نیز در سند **BIS-RG-۳۰۰-۱۴** ذکر کرده است که عبارت‌اند از:

[1] Open Authentication

- رمزهای پویا در طول عمر خود باید تنها یکبار توسط مؤسسه اعتباری پذیرفته شوند.

- رمزهای پویا باید در طول عمر خود صرفاً برای استفاده از خدمات مبتنی بر یک کارت مشخص قابل‌استفاده باشد.

- نباید امکان تولید رمز پویای جدید بر اساس هیچ‌یک از رمزهای پویای پیش‌تر تولیدشده، وجود داشته باشد.

- با افشای یک رمز پویا، نباید هیچ‌گونه اطلاعاتی از عوامل احراز هویت قابل‌استخراج باشد.

- طول نانس[1] مورداستفاده برای تولید رمز پویا باید به‌اندازه‌ای باشد که مؤسسه اعتباری از یکتا ماندن آن در هر عملیات و در تمام طول عمرش اطمینان داشته باشد.

بخش سوم: بررسی کاربردی اپلیکیشن‌های بانک‌ها برای تولید رمزپویا

پس الزامی شدن تدریجی اجرای طرح استفاده از رمز دوم پویا در تراکنش‌های مبتنی بر کارت برای کلیه مشتریان بانک‌های کشور در دی‌ماه ۱۳۹۸، کلیه بانک‌ها و مؤسسات مالی و اعتباری نسبت به تأمین زیرساخت‌ها و ابزارهای لازم برای فعال‌سازی و به‌کارگیری رمز پویا برای مشتریان خود اقدام نمودند. در این مقاله، امکانات مختلف فراهم‌شده در اپلیکیشن تولید رمز پویا توسط بانک‌های کشور از جهات زیر موردبررسی و مقایسه قرارگرفته‌اند:

بند اول: تولید رمز به‌صورت آفلاین و آنلاین

الزام اتصال به اینترنت در اپلیکیشن‌های تولید رمز پویا در برخی از بانک‌ها وجود داشته و در برخی دیگر نیز اپلیکیشن قادر به تولید رمز حتی در حالت آفلاین و بدون ارتباط با اینترنت نیز وجود دارد. برخی از اپلیکیشن‌ها برای تولید رمز پویا وابسته به تاریخ و ساعت تلفن همراه هستند که لزوماً باید با سرور احراز هویت یکسان باشد. این الزام غالباً برای اپلیکیشن‌هایی است که قابلیت

[1] Nounce

تولید رمز به‌صورت آفلاین را نیز دارا می‌باشند. در صورتیکه مشتری نیاز به تولید و استفاده از رمز یکبارمصرف در هنگام سفر به کشورهایی که اختلاف ساعت با ایران دارند داشته باشد، تاریخ و ساعت تلفن همراه باید بر روی تاریخ و ساعت رسمی ایران تنظیم‌شده باشد.

بند دوم: طول رمز پویا

با توجه به اینکه تعداد رقم‌های رمز دوم الزاماً ثابت نیست، طول رمز تولیدشده در بانک‌های مختلف، از ۵ رقم تا ۱۲ رقم متفاوت است. بااین‌حال، الزام بانک مرکزی حداقل ۷ رقم است که برخی از بانک‌ها این الزام را رعایت نکرده‌اند.

بند سوم: اپلیکیشن‌های مستقل برای تولید رمز

برخی از بانک‌ها یک اپلیکیشن مستقل و مجزا برای تولید رمز پویا ارائه کرده‌اند و برخی دیگر نیز با اضافه کردن بخش جدیدی به نرم‌افزار همراه بانک خود، این امکان را برای مشتریان خود فراهم کرده‌اند که استفاده برخی بانک‌ها از روش دوم، مشکلاتی را برای کاربران ایجاد کرده است؛ زیرا در زمان انجام تراکنش با نرم‌افزار همراه بانک، امکان اخذ رمز وجود ندارد لذا قبل از انجام تراکنش باید رمز را دریافت کرده، آن را یادداشت کرده یا به خاطر سپرد و سپس اقدام به انجام تراکنش نمود که در بسیاری از موارد، زمان ۶۰ ثانیه اعتبار رمز مذکور قبل از انجام تراکنش به پایان می‌رسد.

بند چهارم: مدت اعتبار رمز

هرچند که طبق الزام بانک مرکزی، حداکثر مدت‌زمان اعتبار رمز دوم پویا ۶۰ ثانیه است، اما برخی از بانک‌ها در اپلیکیشن خود این قابلیت را پیش‌بینی کرده‌اند که به انتخاب مشتری این زمان از ۳۰ ثانیه تا ۱۲۰ ثانیه قابل‌تغییر باشد.

بند پنجم: قابلیت کپی کردن رمز

قابلیت کپی کردن رمز تولیدشده و چسباندن آن در محل موردنظر در درگاه‌های پرداخت از قابلیت‌های مفیدی است که برخی اپلیکیشن‌ها از آن‌ها بی‌بهره هستند.

بند ششم: قابلیت ارسال رمز پویا با پیامک

هرچند که اکثر مشتریان تمایل به استفاده از رمز پویا پیامکی رادارند اما با توجه به اینکه هزینه آن باید توسط بانک صادرکننده کارت باید پرداخت شود و به مشتری هیچ‌گونه هزینه‌ای نباید تحمیل شود، اغلب بانک‌ها تمایلی به استفاده از این روش ندارند. بااین‌حال تعدادی از بانک‌ها برای رفاه حال مشتریان خود این امکان را نیز فراهم کرده‌اند. بسیاری از مشتریانی که از تلفن همراه هوشمند استفاده نمی‌کنند بسیار مفید می‌تواند باشد.

بند هفتم: قابلیت ارسال رمز پویا از طریق USSD

ارسال رمز پویا از طریق کدهای دستوری علاوه بر اینکه هزینه‌ای برای بانک ندارد، برای بسیاری از مشتریانی که از تلفن همراه هوشمند استفاده نمی‌کنند قابل‌استفاده است که برخی از بانک‌ها این خدمت را نیز ارائه می‌کنند.

بند هشتم: قابلیت ارائه رمز اول پویا

انجام تراکنش باکارت بانکی در پایانه‌های فروش و دستگاه‌های خودپرداز لزوماً با رمز اول ۴ رقمی و به همراه‌کارت بانکی (به‌عنوان عامل دوم احراز هویت) امکان‌پذیر است. هرچند که طبق دستورالعمل بانک مرکزی، ارائه و استفاده از رمز اول پویا اختیاری است اما برخی از بانک‌ها در اپلیکیشن خود، امکان فعال‌سازی و ارائه رمز اول پویا را نیز برای مشتریان خود فراهم کرده‌اند.

بند نهم: روش‌های ورود به اپلیکیشن تولید رمز

طبق ماده ۳۷ سند الزامات رمزهای پویا، برای استفاده از اپلیکیشن تولید رمز، کاربر لزوماً باید با حداقل یکی از روش‌های «دانستنی[1]» مثل کلمه عبور یا الگو و «ویژگی‌های ذاتی[2]» مثل اثرانگشت یا چهره احراز هویت شود.

بند دهم: روش فعال‌سازی رمز پویا

بانک‌ها در اطلاع‌رسانی‌های انجام‌شده برای فعال‌سازی رمز پویا روش‌های مختلفی را اعلام کرده‌اند که با ترکیبی از دو روش حضوری (از طریق شعبه با کنترل مدارک هویتی یا از طریق دستگاه خودپرداز منوط به احراز هویت مبتنی بر کارت‌بانکی و رمز اول) و روش غیرحضوری (مبتنی بر اینترنت و احراز هویت چندعاملی و تأیید کد ارسال‌شده به تلفن همراه دارنده کارت) امکان‌پذیر می‌باشد. آنچه مسلم است، تمایل کاربران به فعال‌سازی بدون نیاز به مراجعه شعبه می‌باشد.

در جدول شماره ۲، امکانات، ویژگی‌ها و متدهای مختلف تولید رمز پویا توسط بانک‌های مختلف به‌طور خلاصه بررسی‌شده است. با بررسی این ویژگی‌ها می‌توان دریافت که برخی از بانک‌ها با تسهیل در فعال‌سازی رمز پویا به روش‌های غیرحضوری و بدون نیاز به مراجعه به شعبه یا دستگاه خودپرداز، امکان ارسال رمز پویا از طریق پیامک یا کدهای دستوری برای مشتریانی که از تلفن همراه هوشمند استفاده نمی‌کنند و فراهم کردن قابلیت‌هایی در اپلیکیشن خود از قبیل امکان کپی کردن رمز، افزایش مدت اعتبار رمز تا ۱۲۰ ثانیه و ورود آسان به اپلیکیشن از طریق روش‌های احراز هویت زیست‌سنجی، به‌کارگیری رمز پویا را برای مشتریان خود تسهیل کرده‌اند که ازجمله این بانک‌ها می‌توان به بانک ملی، بانک ملت و بانک سپه اشاره کرد که در این زمینه پیشتاز هستند.

---

[1] Something You Know

[2] Something You Are

جدول ۲- مقایسه روش‌ها و قابلیت‌های رمز یکبارمصرف بانک‌ها

ردیف	نام بانک	نام اپلیکیشن تولید رمز پویا	آنلاین/آفلاین	طول رمز (تعداد رقم)	اپلیکیشن مستقل برای تولید رمز	قابلیت کپی کردن رمز	مدت اعتبار رمز (ثانیه)	قابلیت ارسال رمز پویا از طریق USSD	قابلیت ارائه رمز اول پویا	نحوه فعال‌سازی رمز پویا	روش‌های ورود به اپلیکیشن تولید رمز
۱	ملی	رمزبان	آفلاین	۷	✓	✓	۶۰/۳۰ /۱۲۰/۹۰	✗	✓	Mobile OTP: اینترنت بانک + پیامک SMS OTP: خودپرداز + USSD	الگو / کلمه عبور
۲	ملت	رمزنگار	آنلاین	۷	✓	✓	۱۲۰	✗	✓	Mobile OTP: خودپرداز + پیامک SMS OTP: خودپرداز	اثرانگشت / کلمه عبور
۳	صادرات	ریما	آفلاین	۷	✓	✓	۶۰	✗	✓	Mobile OTP: خودپرداز + پیامک	اثرانگشت/چهره/کلمه عبور
۴	تجارت	همراز	آفلاین	۸	✓	✓	۶۰/۴۰/۳۰	✓	✗	Mobile OTP: خودپرداز+پیامک USSD :USSD OTP	اثرانگشت / کلمه عبور
۵	پاسارگاد	-	آنلاین	۵	✗	✗	۱۸۰	✗	✗	Mobile OTP: اینترنت بانک + همراه بانک USSD :SMS OTP	اثرانگشت / کلمه عبور
۶	سامان	رمزینه	آفلاین	۶	✓	✗	۶۰	✗	✓	Mobile OTP: اینترنت بانک + پیامک	کلمه عبور

			ین								
۷	آینده	ریما	آفلاین	۷	✓	✓	۶۰	✗	✓	Mobile OTP: خودپرداز + پیامک SMS OTP: خودپرداز + پیامک	اثرانگشت/ کلمه عبور
۸	رسالت	-	آنلاین	۵	✗	✗	۱۸۰	✗	✗	Mobile OTP: اینترنت بانک + همراه بانک	اثرانگشت / کلمه عبور
۹	انصار	آپان	آفلاین	۷	✓	✓	۶۰/۳۰ ۱۲۰/۹۰	✗	✗	Mobile OTP: اینترنت بانک + پیامک	الگو / کلمه عبور
۱۰	رفاه	رمزساز رفاه	آفلاین	۷	✓	✗	۱۲۰	✓	✗	Mobile OTP: خودپرداز + پیامک	اثرانگشت / کلمه عبور
۱۱	پارسیان من	پارسیا من	آفلاین	۷	✗	✗	۱۲۰	✗	✓	Mobile OTP: خودپرداز + پیامک + همراه	اثرانگشت/ کلمه عبور
۱۲	دی	ارس	آفلاین	۶	✓	✓	۶۰/۳۰ ۱۲۰/۹۰	✗	✗	Mobile OTP: اینترنت بانک	الگو / کلمه عبور
۱۳	گردشگری	-	آنلاین	۵	✗	✗	۱۲۰	✗	✗	Mobile OTP: اینترنت بانک	اثرانگشت/ کلمه عبور
۱۴	سپه	رمزساز سپه	آفلاین	۸	✓	✓	۶۰	✓	✗	Mobile OTP: شعبه + پیامک USSD :SMS OTP USSD ◌ USSD : OTP	اثرانگشت / چهره / کلمه عبور
۱۵	شهر	رمزنت	آفلاین	۶	✓	✓	۶۰	✗	✓	Mobile OTP: اینترنت بانک + پیامک	اثرانگشت / کلمه عبور
۱۶	مسکن	رمزنما	آفلاین	۸	✓	✓	۶۰	✗	✓	Mobile OTP: خودپرداز + پیامک SMS OTP: خودپرداز + پیامک	اثرانگشت / کلمه عبور

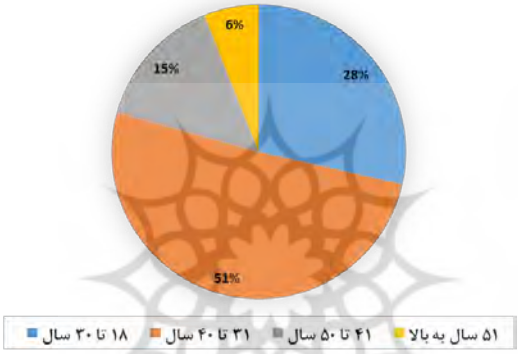
۱۷	اقتصاد نوین	ارس	آفلاین	۶	✓	✓	/۶۰/۳۰ ۱۲۰/۹۰	✓	✗	✓	Mobile OTP: اینترنت بانک	الگو / کلمه عبور
۱۸	قوامین	جی بی رمز	آفلاین	۱۲ ـ۷	✓	✗	۶۰	✓	✗	✓	Mobile OTP: خودپرداز + پیامک	کلمه عبور
۱۹	سرمایه	رمزساز سرمایه	آنلاین	۶	✓	✗	۶۰	✓	✗	✓	Mobile OTP: اینترنت بانک + پیامک	کلمه عبور
۲۰	سینا	ارس	آفلاین	۶	✓	✓	/۶۰/۳۰ ۱۲۰/۹۰	✗	✗	✓	Mobile OTP: اینترنت بانک + پیامک	الگو / کلمه عبور

بخش چهارم: پرسشنامه سنجش میزان رضایتمندی مشتریان بانک‌ها از رمز دوم پویا

در اجرای یک طرح ملی که کلیه اقشار جامعه با آن سروکار دارند، تمامی جوانب آن باید سنجیده شود. طرح حذف رمز دوم ثابت و الزام استفاده از رمز دوم پویا برای تراکنش‌های بانکی بدون کارت، ازجمله طرح‌هایی است که انتقاداتی به آن در بین مشتریان بانک‌ها مطرح‌شده است. مشکلاتی که در استفاده از رمز دوم پویا برای اقشاری از جامعه ازجمله سالمندان، افراد فاقد تحصیلات کافی و افرادی که از تلفن همراه هوشمند استفاده نمی‌کنند حائز اهمیت است. در این تحقیق، یک نظرسنجی از میان ۳۸۲ نفر از اقشار مختلف جامعه انجام‌شده است تا میزان رضایتمندی آن‌ها از طرح الزام استفاده از رمز دوم پویا مورد ارزیابی قرار گیرد. فرم این نظرسنجی شامل ۱۸ سؤال و مبتنی بر پلتفرم Google Form طراحی در شبکه‌های اجتماعی منتشرشده است، لذا فرض بر این است که کلیه شرکت‌کنندگان در این نظرسنجی از تلفن همراه هوشمند استفاده می‌کنند. جامعه آماری در این تحقیق شامل ۲۲۸ نفر مرد (۶۰ درصد) و ۱۵۴ نفر زن (۴۰ درصد) می‌باشد. محدوده سنی افراد شرکت‌کننده در این نظرسنجی در جدول شماره ۳ و سطح تحصیلات آن‌ها در جدول شماره ۴ آمده است. همچنین در جدول شماره ۵، تعداد کارت‌های بانکی فعال افراد شرکت‌کننده در این نظرسنجی ذکرشده است.

جدول شماره ۳- محدوده سنی شرکت‌کنندگان در نظرسنجی

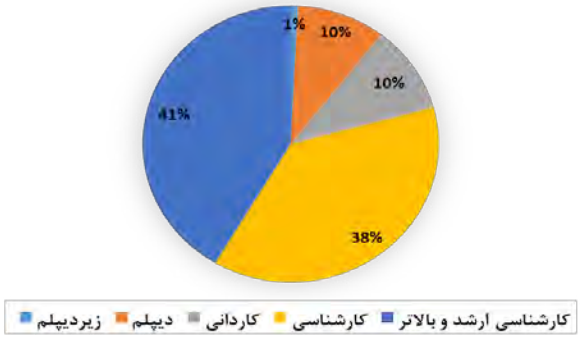
محدوده سنی	تعداد شرکت‌کنندگان	درصد شرکت‌کنندگان
۱۸ تا ۳۰ سال	۱۰۹	۲۸
۳۱ تا ۴۰ سال	۱۹۴	۵۱
۴۱ تا ۵۰ سال	۵۶	۱۵
۵۱ سال به بالا	۲۳	۶



شکل ۱ – نمودار توزیع محدوده سنی شرکت‌کنندگان در نظرسنجی

جدول شماره ۴- میزان تحصیلات شرکت‌کنندگان در نظرسنجی

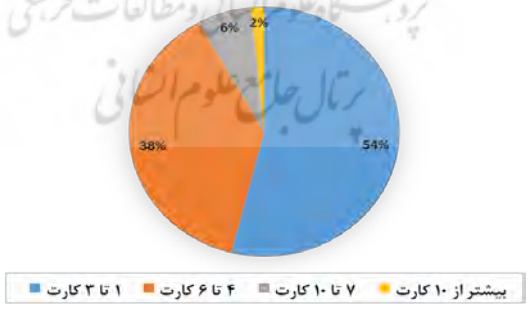
تحصیلات	تعداد شرکت‌کنندگان	درصد شرکت‌کنندگان
زیر دیپلم	۳	۱
دیپلم	۳۷	۱۰
کاردانی	۳۹	۱۰
کارشناسی	۱۴۴	۳۸
کارشناسی ارشد و بالاتر	۱۵۸	۴۱



شکل ۲ – نمودار توزیع سطح تحصیلات شرکت‌کنندگان در نظرسنجی

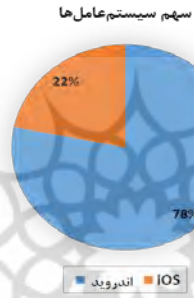
جدول شماره ۵ – تعداد کارت‌های بانکی فعال شرکت‌کنندگان در نظرسنجی

تعداد کارت‌های بانکی فعال	تعداد شرکت‌کنندگان	درصد شرکت‌کنندگان
۱ تا ۳ کارت	۲۰۶	۵۴
۴ تا ۶ کارت	۱۴۵	۳۸
۷ تا ۱۰ کارت	۲۵	۶
بیشتر از ۱۰ کارت	۶	۲

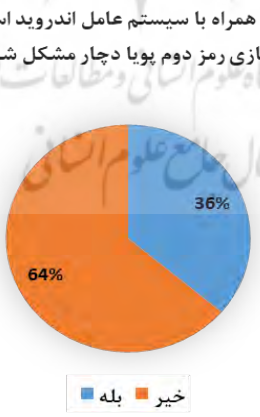


شکل ۳– نمودار توزیع تعداد کارت‌های بانکی فعال شرکت‌کنندگان در نظرسنجی

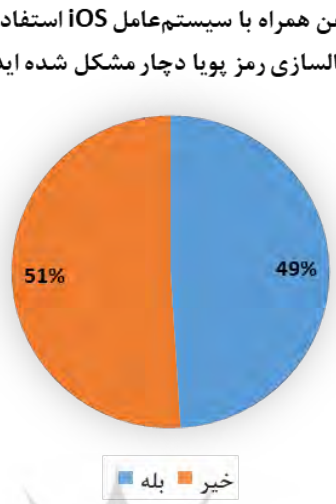
جهت سنجش عملکرد اپلیکیشن‌های ارائه‌شده برای تولید رمز پویا در سیستم‌عامل‌های مختلف، از کاربران سیستم‌عامل‌های اندروید و **iOS** پرسیده شده است که نسبت پاسخ‌ها در شکل‌های ۴ و ۵ نشان داده‌شده است؛ که تلفن همراه ۷۸ درصد این افراد مجهز به سیستم‌عامل اندروید و ۲۲ درصد مجهز به سیستم‌عامل **iOS** می‌باشد. همان‌طور که قابل پیش‌بینی بود، تنها ۳۶ درصد کاربران اندروید در فعال‌سازی اپلیکیشن‌های تولید رمز دوم پویا به مشکل مواجه شده‌اند درحالی‌که این نسبت در کاربران **iOS** ۴۹ درصد است که عمدتاً به دلایل فنی و محدودیت‌های اعمال‌شده توسط شرکت اپل برای کاربران ایرانی است.



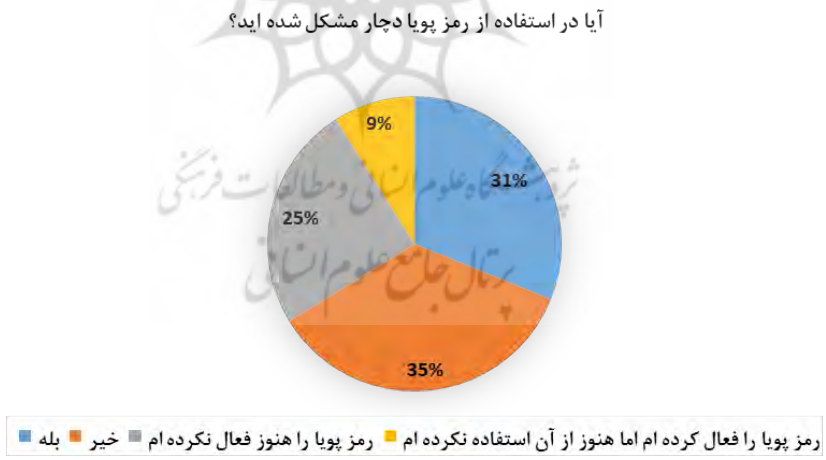
شکل ۴- سهم سیستم‌عامل‌ها



شکل ۵- نسبت کاربرانی که در فعال‌سازی رمز پویا در سیستم‌عامل اندروید با مشکل مواجه شده‌اند

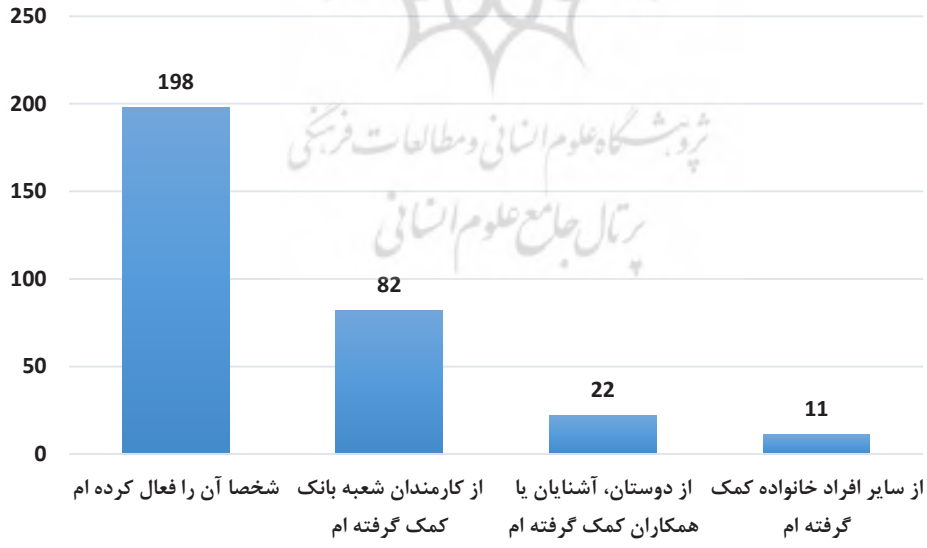


شکل ۶- نسبت کاربرانی که در فعال‌سازی رمز پویا در سیستم‌عامل iOS با مشکل مواجه شده‌اند

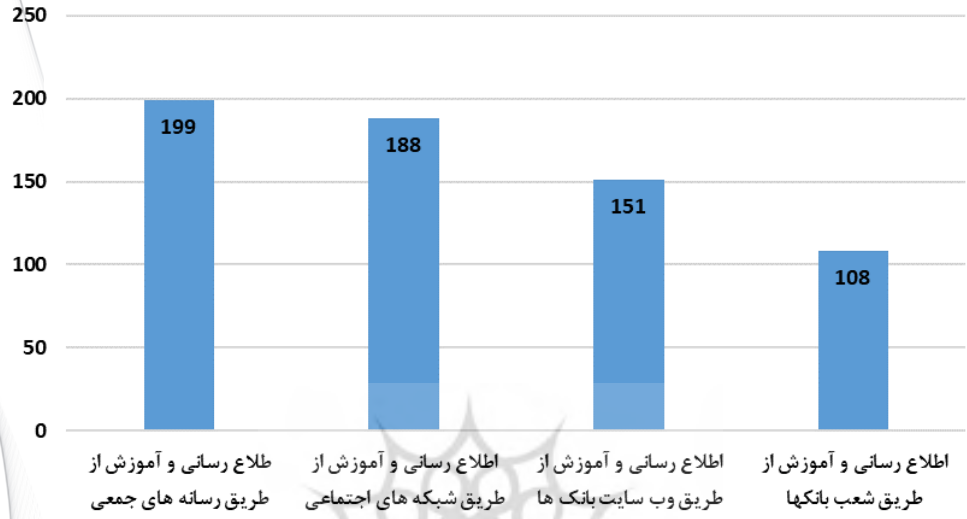


شکل ۷- پاسخ‌های کاربران به پرسشی درباره مواجهه با مشکل در استفاده از رمز دوم پویا

اطلاع‌رسانی، آموزش و فرهنگ‌سازی در اجرای طرح‌های همگانی از مهم‌ترین چالش‌های پیش روی متولیان آن است و در صورتیکه آموزش‌های لازم و کافی به مخاطبان داده نشود اجرای هر طرح ملی را با مشکل مواجه ساخته و موجبات نارضایتی کاربران آن را نیز به دنبال دارد. الزام استفاده از رمز دوم پویا در تراکنش‌های بدون کارت نیز ازجمله طرح‌های مفید و مؤثر در افزایش امنیت تراکنش‌های بانکی است اما به دلیل عدم اطلاع‌رسانی و آموزش مناسب و فراهم نبودن زیرساخت‌های لازم اجرای قطعی آن بار ها به تعویق افتاده است. مطابق شکل شماره ۸، بااینکه ۱۹۸ نفر (۶۸ درصد پاسخ‌دهندگان) شخصاً رمزدوم پویا را بر روی تلفن همراه خود نصب و فعال‌سازی کرده‌اند اما ۶۶ درصد از شرکت‌کنندگان در این نظرسنجی بر این باور هستند که نحوه اطلاع‌رسانی و آموزش استفاده از رمز دوم پویا کافی و مناسب نبوده است و استفاده از رسانه‌های جمعی از قبیل رادیو، تلویزیون و نشریات را از بهترین روش‌های آموزش و اطلاع‌رسانی را که مناسب تشخیص داده‌اند. میزان محبوبیت سایر روش‌ها نیز در شکل ۹ نشان داده‌شده است.



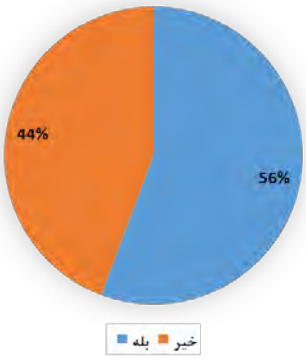
شکل ۸ – روش‌های استفاده‌شده برای فعال‌سازی رمز پویا توسط کاربران



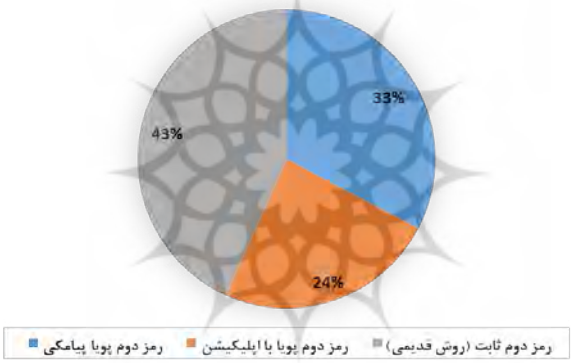
شکل ۹- میزان محبوبیت روش‌های آموزش و اطلاع‌رسانی

برای سنجش میزان مقبولیت استفاده از رمز پویا در بین مشتریان بانک‌ها، ۴ سؤال از شرکت‌کنندگان در نظرسنجی پرسیده شده است که به همراه میزان پاسخ‌ها در ادامه نشان داده‌شده است.

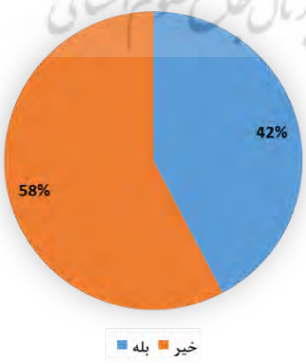
- آیا موافق اجرای استفاده از رمز پویا برای افزایش امنیت تراکنش‌های مالی هستید؟



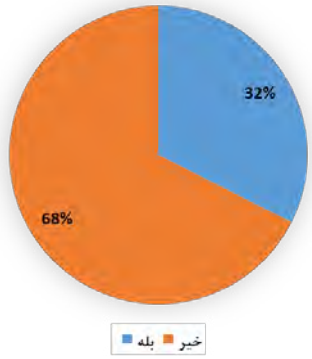
- استفاده از کدام روش را ترجیح می‌دهید؟



- در صورتیکه استفاده از رمز پویا اختیاری باشد آیا بازهم از آن استفاده می کنید؟

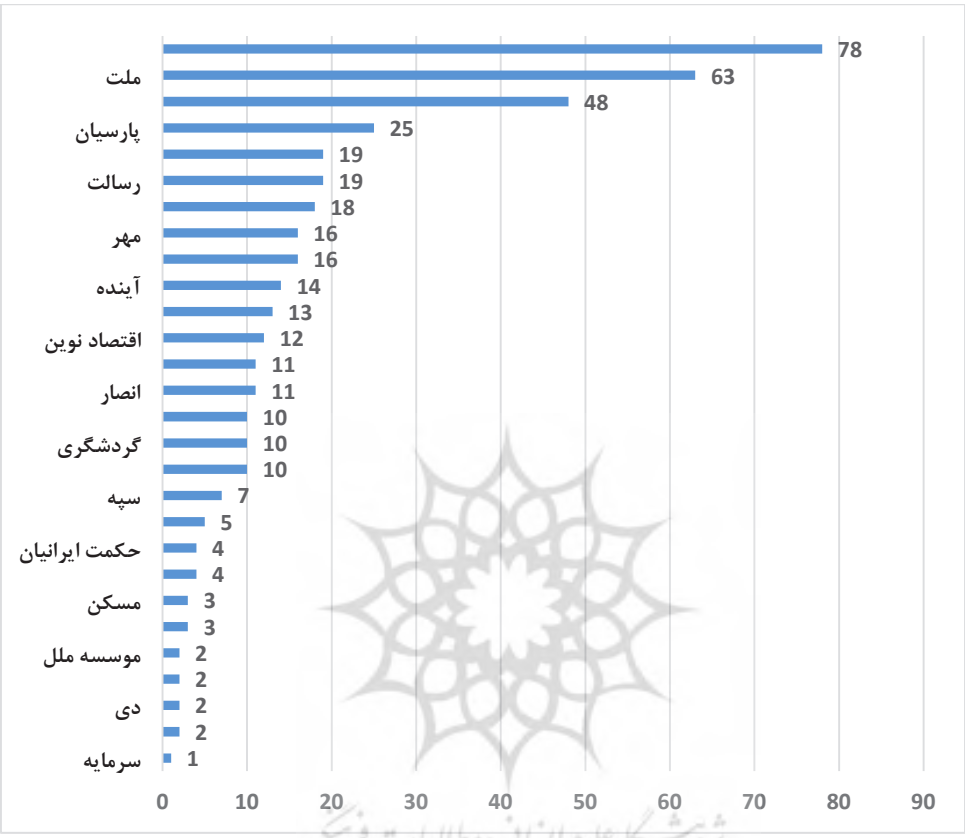


- آیا زمان ۶۰ ثانیه به‌عنوان مدت اعتبار رمز برای شما کافی است؟



بخش پنجم: انتخاب بانک‌ها و مؤسسات مالی و اعتباری توسط مشارکت‌کنندگان در نظرسنجی

در آخرین پرسش، از کاربران خواسته‌شده است تا بر اساس تجربه خود، بانک‌هایی را که بهترین روش فعال‌سازی رمز یکبارمصرف را داشته‌اند انتخاب کنند. هرچند که انتظار می‌رفت بانک‌های دولتی به دلیل اینکه که مشتریان زیادی دارند در صدر قرار گیرند، اما پاسخ‌ها نشان می‌دهد بعد از دو بانک ملی و ملت، بانک‌های پاسارگاد و پارسیان در جایگاه سوم و چهارم رضایت مشتریان قرارگرفته‌اند و سایر بانک‌های دولتی از قبیل صادرات، سپه، تجارت و مسکن علیرغم اینکه تعداد مشتریان بیشتری نسبت به بانک‌های خصوصی دارند اما رتبه قابل قبولی در این نظرسنجی کسب نکرده‌اند. شکل ۱۴، میزان رضایت مشتری‌ان از فرآیند فعال‌سازی رمز دوم پویا و امکانات ارائه‌شده در اپلیکیشن تولید رمز یکبارمصرف بانک‌ها را نشان می‌دهد.



شکل ۱۴ - میزان رضایت مشتریان از فرآیند فعال‌سازی رمز دوم پویا و امکانات ارائه‌شده در اپلیکیشن تولید رمز یکبارمصرف بانک‌ها

نتیجه‌گیری

سؤالات این نظرسنجی را در سه حوزه بررسی قابلیت‌های فنی، فرهنگ‌سازی و آموزش و میزان مقبولیت عمومی می‌توان دسته‌بندی نمود. در حوزه قابلیت‌های فنی نرم‌افزارهای تولید رمز یکبارمصرف، از پاسخ‌های داده‌شده به سؤالات می‌توان نتیجه گرفت که صرف‌نظر از نوع سیستم‌عامل، بیش از ۳۰ درصد کاربران در فعال‌سازی و استفاده از رمز دوم پویا با مشکلاتی مواجه

شده‌اند که باعث نارضایتی آن‌ها شده است. بدیهی است هر سامانه جدیدی در ابتدای راه با مشکلات فنی مواجه خواهد شد که باگذشت زمان و ارائه نسخه‌های به‌روزرسانی شده توسط بانک‌ها بهبود خواهد یافت.

در حوزه فرهنگ‌سازی و آموزش، نارضایتی بالایی از نحوه آموزش و اطلاع‌رسانی وجود داشته و مشتریان بانک‌ها انتظار دارند محتوای آموزشی برای فعال‌سازی و استفاده از رمز دوم پویا در رسانه‌های جمعی پرمخاطب از قبیل رادیو، تلویزیون و نشریات و شبکه‌های اجتماعی که در اختیار مخاطبان قرار گیرد تا بتوانند شخصاً و بدون کمک گرفتن از سایر افراد، نرم‌افزارهای تولید رمز پویا را نصب و بهره‌برداری کنند.

در حوزه مقبولیت عمومی، علیرغم اینکه ۵۶ درصد افراد موافق اجرای طرح رمز دوم پویا هستند اما دشواری‌هایی که استفاده از این طرح برای مردم به وجود آورده است از قبیل کوتاه بودن مدت اعتبار رمز پویا (۶۰ ثانیه) و نیاز به نصب تعداد زیادی اپلیکیشن برای بانک‌های مختلف، مشتریان بانک‌ها همچنان ترجیح می‌دهند از رمز ثابت استفاده کنند.

انتقادات و پیشنهادات

در پرسشنامه، بخشی برای درج پیشنهادها در نظر گرفته‌شده بود که پاسخ‌های حائز اهمیتی از ۶۴ نفر دریافت گردید که کلیه مشارکت‌کنندگان از اجرای این طرح به دلایل زیر نارضایتی خود را اعلام کرده بودند:

- نصب اپلیکیشن‌های متعدد که منجر به سردرگمی و اشغال حافظه تلفن همراه می‌شود.
- عدم همکاری و پاسخگویی مناسب کارمندان شعب بانک‌ها و کارشناسان سامانه‌های پاسخگویی تلفنی

- کوتاه بودن مدت‌زمان اعتبار رمز یکبارمصرف
- مشکل انجام تراکنش‌های بانکی برای افراد فاقد تلفن همراه هوشمند و عدم وجود سرویس پیامکی رمز پویا در اکثر بانک‌ها
- ایجاد مشکل برای افراد کم‌سواد و مسن که منجر به مراجعه حضوری به شعب برای انجام عملیات بانکی خواهد شد
- مشکلات فنی به وجود آمده برای کاربرانی که از تلفن همراه آیفون استفاده می‌کنند
- روش فعال‌سازی و استفاده از آن بسیار سخت و پردردسر است
- استفاده از اپلیکیشن تولید رمز پویا برای پرداختهای مبتنی بر USSD امکان‌پذیر نیست

و برای رفع برخی از مشکلاتی که در هنگام فعال‌سازی و استفاده از رمز پویا با آن مواجه شده بودند پیشنهادهای زیر را مطرح کرده‌اند:

- استفاده از رمز دوم یکبارمصرف اختیاری باشد
- برای پرداخت‌های بیشتر از حد معینی استفاده از رمز پویا الزامی باشد و تراکنش‌های خُرد با استفاده از رمز دوم ثابت انجام شود
- یک اپلیکیشن متمرکز برای کلیه بانک‌ها ارائه شود
- رمز دوم یکبارمصرف از طریق پیامک ارسال شود

منابع و مآخذ

[۱] م. شمس, "میزان فیشینگ نسبت به مدت مشابه سال گذشته با رشد مواجه بوده است / با اجرای رمز دوم یک‌بار مصرف فیشینگ به صفر می‌رسد," ۲۰ آبان ۱۳۹۸

[۲] "رمز پویا با رمز یک بار مصرف بانکی چیست؟ " آبان ۱۳۹۸ ۱۸

[3] Cryptomathic, "Two-Factor Authentication for Banking " White Paper October 2012 2012. [Online]. Available: www.cryptomathic.com

[4] C. Cimpanu, "Microsoft: Using multi-factor authentication blocks 99.9% of account hacks," Security August 27, 2019 2019. [Online]. Available: https://www.zdnet.com/article/microsoft-using-multi-factor-authentication-blocks-99-9-of-account-hacks/.

[5] "Frequently Asked Questions on FFIEC Guidance on Authentication in an Internet Banking Environment " August 15, 2006 [Online]. Available:https://www.ffiec.gov/pdf/authentication_faq.pdf.

[6] J. Davis, "Two Factor Auth (2FA)." [Online]. Available: https://twofactorauth.org/#banking.

[8] D. M'Raihi, "An HMAC-Based One-Time Password Algorithm," Network Working Group Informational December 2005. [Online]. Available: https://tools.ietf.org/html/rfc4226.

[9] M. Stevens, E. Bursztein, P. Karpman, A. Albertini, and Y. Markov, "The First Collision for Full SHA-1," in International Conference on Information Technology: New Generations, ITNG 2017, pp. 570-596, doi: 10.1007/978-3-319-63688-7_19 .

[10] C. A. Soare, "Internet Banking Two-Factor Authentication using Smartphones," 2012 .

[11] D. M'Raihi, "TOTP: Time-Based One-Time Password Algorithm," Internet Engineering Task Force (IETF) May 2011. [Online]. Available: https://tools.ietf.org/html/rfc6238.