

راهنمای امنیت اینستاگرام 🗝️

آموزش کامل امن سازی اکانت اینستاگرام در ۲۰۲۶

۱۰ قدم طلایی برای جلوگیری از هک شدن + چک لیست کامل

نسخه کتابچه — savisgame.com

فهرست مطالب

1. استفاده از Password Manager معتبر
2. ساخت رمز عبور کاملاً اختصاصی برای اینستاگرام
3. فعال سازی احراز هویت دو مرحله ای (2FA)
4. انتخاب و تنظیم اپلیکیشن Authenticator
5. وارد کردن کد ۶ رقمی و تکمیل فعال سازی
6. ذخیره Recovery / Backup Codes
7. نکات امنیتی قبل از تعویض گوشی
8. شناسایی و مقابله با فیشینگ
9. بررسی دستگاه های وارد شده به اکانت
10. بررسی اپ ها و سرویس های متصل
11. ۵ نکته تکمیلی
12. چک لیست نهایی امنیت اینستاگرام
13. پرسش های پرتکرار

فقط یک رمز عبور قوی، دیگر کافی نیست. هر روز هزاران اکانت اینستاگرام هک می شوند؛ نه چون هکرها رمزها را می شکنند، بلکه چون یک رمز تکراری، یک لینک فیشینگ، یا یک اپلیکیشن مشکوک کافی است تا کنترل اکانت از دستتان خارج شود. در این کتابچه، اکانت اینستاگرام مان را به صورت چندلایه امن می کنیم.

۱. اول یک Password Manager داشته باش

به جای استفاده از یک رمز مشترک برای همه حساب‌هایت، از یک مدیریت‌کننده رمز عبور معتبر کمک بگیر. این ابزارها برای هر سرویس یک رمز تصادفی و منحصر به فرد می‌سازند و ذخیره می‌کنند.

• Bitwarden — رایگان و متن‌باز

• Proton Pass — ادغام شده با اکوسیستم Proton

۲. رمز عبور کاملاً اختصاصی برای اینستاگرام

با کمک Password Manager یک رمز تصادفی و منحصر به فرد فقط برای اینستاگرام بساز.

✕ استفاده نکن از: 123456789، Instagram123، اسم+تاریخ تولد، یا رمز مشترک با ایمیل.

● رمز اینستاگرام نباید با ایمیل، تلگرام، فیسبوک یا سرویس دیگری یکسان باشد.

۳. فعال سازی 2FA

مسیر: Two-factor authentication ← Password and security ← Accounts Center ← ≡ ← Profile، سپس گزینه Authentication app را انتخاب کن.

۴. انتخاب اپلیکیشن Authenticator

گزینه‌های پیشنهادی: Google Authenticator، Microsoft Authenticator، 2FAS، Aegis، QR Code را با اپ اسکن کن یا Setup Key را دستی وارد کن.

۵. وارد کردن کد ۶ رقمی

کد تولید شده توسط Authenticator را وارد کن تا 2FA فعال شود. از این پس هر بار برای ورود، رمز عبور + کد Authenticator لازم است.

۶. مهم ترین مرحله: Recovery Codes

🔥 خیلی ها همین جا اشتباه می کنند و بعداً پشیمان می شوند.

بلافاصله بعد از فعال کردن 2FA، Backup / Recovery Codes را دریافت و در محلی امن ذخیره کن. این کدها در این شرایط نجات بخش اند: گم شدن گوشی، خرابی گوشی، پاک شدن Authenticator، تعویض گوشی، یا عدم دسترسی به کد 2FA.

⚠ Recovery Code یا کد Authenticator را برای هیچ کس ارسال نکن؛ حتی اگر خودش را «پشتیبانی اینستاگرام» معرفی کند.

۷. قبل از تعویض گوشی

✓ مطمئن شو Authenticator روی گوشی جدید فعال شده، ورود را تست کن و Recovery Codes را در دسترس داشته باش — سپس گوشی قدیمی را ریست کن.

۸. مقابله با فیشینگ

پیام هایی مثل «اکانت شما گزارش شده»، «در حال مسدود شدن است»، یا «این کد را برای تأیید ارسال کنید» معمولاً تلاش برای فریب دادن شماست.

● رمز، کد Authenticator و Recovery Code را به هیچ کس نده. قبل از کلیک روی لینک، از اصالت آن مطمئن شو.

۹. بررسی دستگاه های وارد شده

هر چند وقت یک بار دستگاه های متصل را چک کن. در صورت مشاهده ورود ناشناس: از آن دستگاه خارج شو، رمز را عوض کن و 2FA را بررسی کن.

۱۰. اپ های متصل به اکانت

مراقب سرویس های «بین کی پروفایل را دیده» یا «فالور رایگان» باش؛ این ها معمولاً دسترسی کامل به اکانت می گیرند. دسترسی های غیرضروری را حذف کن.

۵ نکته تکمیلی که خیلی‌ها نادیده می‌گیرند

۱. ایمیل و شماره بازیابی را هم امن کن

روی ایمیل اصلی که برای بازیابی اینستاگرام استفاده می‌شود هم 2FA فعال کن.

۲. Login Alerts را فعال کن

برای دریافت هشدار فوری در صورت ورود ناشناس.

۳. روی وای‌فای عمومی مراقب باش

بدون VPN معتبر وارد اینستاگرام از وای‌فای رایگان نشو.

۴. اپ و سیستم عامل را به‌روز نگه دار

بسیاری از حملات از آسیب‌پذیری‌های قدیمی که در نسخه‌های جدید رفع شده‌اند سوءاستفاده می‌کنند.

۵. برای پیج‌های تجاری جدی‌تر باش

یک ادمین ثانویه جدا تعریف کن و رمز اصلی را در چت‌ها ارسال نکن.

چک‌لیست نهایی امنیت اینستاگرام

- ☐ نصب یک Password Manager معتبر
- ☐ ساخت رمز کاملاً اختصاصی برای اینستاگرام
- ☐ ذخیره رمز داخل Password Manager
- ☐ فعال‌سازی 2FA
- ☐ استفاده از Authenticator
- ☐ ذخیره Recovery Codes در محل امن
- ☐ بررسی دستگاه‌های وارد شده
- ☐ حذف اپ‌های ناشناس متصل
- ☐ عدم کلیک روی لینک‌های مشکوک
- ☐ عدم ارسال رمز/کد امنیتی برای دیگران
- ☐ فعال‌سازی 2FA روی ایمیل بازیابی
- ☐ فعال‌سازی Login Alerts

پرسش‌های پرتکرار

آیا 2FA پیامکی (SMS) کافی است؟

بهتر از هیچ چیز است، اما در برابر SIM Swap آسیب‌پذیر است. Authentication App امنیت بالاتری دارد.

اگر Authenticator را پاک کردم یا گوشی را گم کردم؟

با Recovery Codes می‌توانی بدون Authenticator وارد شوی و 2FA را دوباره تنظیم کنی.

آیا Password Manager امن است؟

بله، با ابزارهای معتبر مثل Bitwarden یا Proton Pass و یک Master Password قوی.

هر چند وقت رمز را عوض کنم؟

مهم‌تر از تعویض دوره‌ای، قوی و منحصر به فرد بودن رمز و فعال بودن 2FA است. فقط در صورت فعالیت مشکوک، فوراً عوض کن.

امنیت اکانت یک اقدام یک‌باره نیست؛ یک عادت همیشگی است. 🗝️

ممنون که این کتابچه را خواندی 🙌

برای مطالب بیشتر درباره امنیت دیجیتال، بازی و ابزارهای کاربردی، سری بزن به:

savisgame.com