

08:33

Захищаємо смартфон і фінансовий номер від шахраїв - поради ПриватБанку

Як убезпечити мобільний пристрій та SIM-картку, щоб зловмисники не дістались до банківських рахунків



Ольга Палій
РЕДАКТОР



Юлія Дюдун
РЕДАКТОР



Як захистити смартфон від шахраїв

Втратити доступ до банківського рахунку можна не лише через необережність в інтернеті, а й через незахищений смартфон або SIM-картку. [Шахраї, що полують на клієнтів ПриватБанку](#), постійно вдосконалюють методи злому - від дзвінків нібито від служби безпеки до перехоплення одноразових паролів. Банк підготував детальні рекомендації: що саме захищати і як діяти, якщо щось пішло не так.

Рекомендації охоплюють два ключові напрями, як зазначає [ПриватБанк](#): захист самого пристрою та захист фінансового номера телефону. Обидва однаково важливі, бо смартфон з незахищеною SIM-карткою - готовий інструмент у руках зловмисника.

Як убезпечити пристрій

Перший рівень захисту - блокування самого гаджета. Варто налаштувати на смартфоні або планшеті пароль, ПІН-код чи графічний ключ. Якщо пристрій опиниться в чужих руках без захисту, зловмисник отримає доступ до SMS-банкінгу та одноразових паролів для Приват24.

Щоб не заразити пристрій вірусами, банк рекомендує:

- користуватися лише **ліцензійною операційною системою**;
- уникати підозрілих сайтів і посилань;
- встановлювати застосунки виключно з App Store або Play Market.

Окремо варто дотримуватися простого правила - не передавати телефон стороннім особам. Навіть короткий доступ до розблокованого пристрою дозволяє шахраю здійснити платіж або змінити налаштування безпеки.

Як захистити фінансовий номер

Фінансовий номер - той, що прив'язаний до банківських рахунків, - потребує окремого рівня захисту. Для цього рекомендують такі кроки:

- встановити **ПІН-код для SIM-картки** (він відрізняється від PIN для розблокування екрана);
- замінити стандартний пароль SIM-картки на власний - це вбереже номер у разі крадіжки телефону;
- звернутися до відділення мобільного оператора та додати до номера дані власника і копію паспорта - це ускладнить перевипуск картки шахраями.

Якщо телефон загубили або вкрали - необхідно діяти швидко. Спочатку зателефонуйте до банку на номер 3700 (безкоштовно з мобільного) і заблокуйте картку та номер телефону. Потім зверніться до мобільного оператора для блокування SIM-картки.

Що робити, якщо шахраї вже зателефонували

Якщо невідомі телефонували і намагалися отримати CVV2-код, пароль або ПІН-код - це привід негайно повідомити банк. Зробити це можна кількома способами. У застосунку Приват24 алгоритм такий:

1. Перейдіть у меню "Комунікації" у правому верхньому куті.
2. Натисніть "Повідомити про шахрайство".
3. Виберіть ситуацію, що трапилася.
4. Зазначте номер, з якого телефонували шахраї, і натисніть "Продовжити".
5. Вкажіть картку, щодо якої розголосили інформацію.
6. Опишіть ситуацію детальніше та натисніть "Продовжити".
7. Дотримуйтеся рекомендацій на екрані.

Також подати звернення можна за телефоном 3700, у чаті "[Допомога Онлайн](#)" або у відділенні банку.

Фото: ПриватБанк

Схеми зловмисників та їхні цілі

Зловмисники представляються працівниками банків, повідомляють, що старий застосунок більше не працює, і надсилають фішингові посилання нібито на офіційний чат-бот у месенджерах. Мета - отримати авторизаційні дані клієнта, а потім переконати назвати код із SMS. Так вони здобувають повний доступ до інтернет-банкінгу і виводять кошти.

Шахраї можуть підмінити номер телефону так, що на екрані відображається нібито офіційний номер банку. Тому найнадійніший захист - не передавати жодних кодів та паролів навіть тому, хто здається співробітником банку. Пам'ятайте: справжні працівники ніколи не запитують ПІН-код або CVV2 першими.

Перевипуск SIM-карток та інші загрози

Якщо виникає підозра, що SIM-картку хочуть перевипустити без відома власника, необхідно негайно звернутися до служби підтримки мобільного оператора. Варто повідомити про підозрілу активність та заблокувати можливість віддаленого перевипуску. Більше про те, як [захиститися від перевипуску SIM-картки](#), описано в матеріалі про цю популярну схему.

Метою зловмисників є доступ до банківських рахунків, BankID, Google-акаунта, пошти та месенджерів для крадіжки коштів або шантажу. Співробітники ПриватБанку ніколи не запитують номер картки, термін дії, ПІН-код чи CVV2-код і не телефонують першими для уточнення особистої інформації. Детальніше про [підступні схеми карткових шахраїв](#) у ПриватБанку читайте в окремому матеріалі.

СЛІДКУЙТЕ ЗА НАМИ У TELEGRAM

Оперативні новини та розбори: Україна, світ, війна

ПІДПИСАТИСЯ

09:06
Фахівці готуються до відключення світла влітку – визначено фактор, який усе вирішить

08:33
 Захисцям смартфон і фінансовий номер від шахраїв - поради ПриватБанку

07:53
 Захисникам та їхнім родинам тепер можна подати одну заяву на кілька державних послуг у Дії

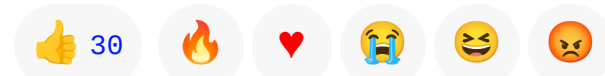
08:53
Податкова знижка за благодійність - українці можуть повернути частину ПДФО

08:03
 Дружина голови Мінцифри пояснила скарги в декларації - Подарунки були дійсно, це нормально абсолютно

07:49
 Україна готує повітряний сюрприз - нову ракету DART запускатимуть зі стратосферних аеростатів

ЧИТАЙТЕ ТАКОЖ:

- [В'язні Чернігівського СІЗО отримали додатково від 7 до 10 років тюрми - виманювали гроші у військових, їхніх родин та волонтерів](#)
- [Забув погасити кредитний ліміт і заплатив на третину більше, ніж взяв - рішення суду](#)
- [Фінансове шахрайство у 2026 році - найнебезпечніші схеми та стратегія захисту](#)



ПРИВАТБАНК | ШАХРАЙСТВО

Світ	Україна	Київ	Регіони	Гроші	Шоу-Біз	Життя
Геополітика	Війна	Столиця	Дніпро	Підвищення податків	Приватне життя	Життя
Країни світу	Події	Влада	Кривий Ріг	Економічне бронювання		Наука
Українці за кордоном	Політика	Бюджет	Нікополь			Здоров'я
	Кримінал	Культура	Буча - Ірпінь			Гороскопи
		Дива	Переяслав			
		Прес-релізи	Івано-Франківськ			
			Коломия			
			Калуш			



Про нас Наші автори Реклама

Інформатор проекти Столиця Ваші фінанси Авто Бек