Как банкам заработать деньги на фроде или ШАХ и МАТ хакерам в 3 хода

КАН Дмитрий
kan.dmitriy@gmail.com

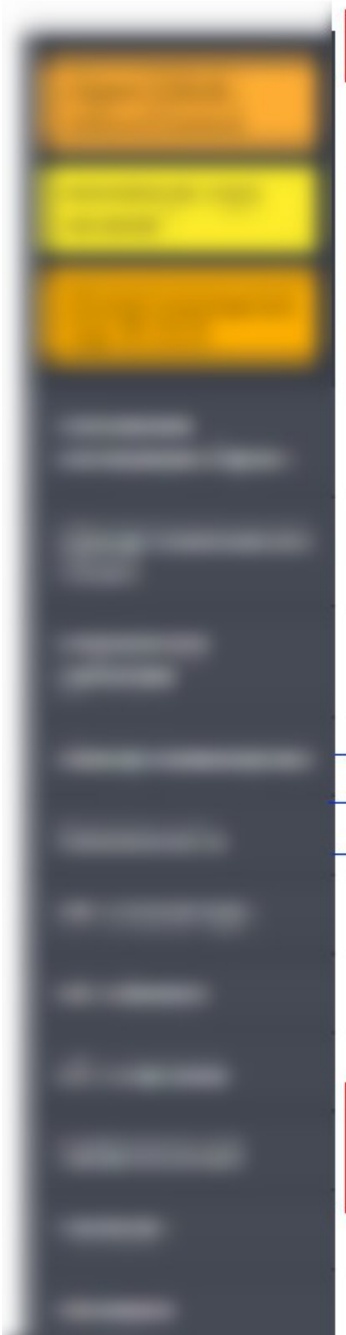
#crystallization

#coldstoragephone
#FIDO.U2F
#VERTU

План презентации:

- объёмы и структура фрода;
- как обманывают мошенники;
- почему всё дело в кнопке?
- ликвидируем фишинг КАК КЛАСС;
- как сделать ШАХ и МАТ хакерам в 3 хода?
- как банкам заработать деньги на фроде?

#killphishermode



26 апреля 2023 12:28 | 6165 | ПОДЕЛИТЬСЯ

Cisco: Пользователи ПК беззащитны перед хакерами, вооруженными ChatGPT

Cisco поделилась опасениями, связанными с использованием хакерами ИИ в фишинговых атаках. В компании отметили, что фишинг становится более персонализированным, а для распознавания атак нового поколения потребуется внедрение новых средств киберзащиты.

ChatGPT в помощь хакерам

Cisco Systems опубликовала предупреждение о том, что программное обеспечение с ИИ значительно усложнит выявление попыток фишинговых атак и потребует от компаний внедрения новых средств киберзащиты. Об этом сообщил Bloomberg со ссылкой на слова вице-президента Cisco **Джиту Патель** (Jeetu Patel), возглавляющего подразделение безопасности Security and Applications business group.

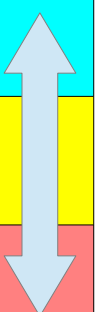
К такому ПО можно отнести ChatGPT разработки OpenAI, а с недавних пор и ранее анонсированный GigaChat Сбербанка.

В компании отметили, что около 80% всех случаев получения незаконного доступа к компьютерным системам достигается посредством фишинга, когда хакеры рассылают электронные письма или текстовые сообщения людям, надеясь обманом заставить их открыть вредоносную ссылку.

Объём и структура фрода:

– 15 млрд тенге в 2022 / 3 млрд в 2023;

	АРРФР	др. источники
Проникновение	55,80%	77,00%
Вишинг телефонные мошенники	34,20%	90,00%
Фишинг	32,70%	8,00%
Whailing / hacking		2,00%
Финансовые пирамиды	21,60%	
Платёжные карты	11,50%	



#how2%whailingmakes90%vishing

Существующие «бумажные» правила ИБ
не обеспечивают безопасность при компрометации смартфона / web-терминала клиента.

Позиция банков: клиенты не соблюдают правила ИБ

Мнение экспертов: есть уязвимости нулевого дня.

Уязвимость нулевого дня

Материал из Википедии — свободной энциклопедии [править | править код]

0-day (англ. *zero day*) — термин, обозначающий неустранённые уязвимости, а также вредоносные программы, против которых ещё не разработаны защитные механизмы.[1]

«Безопасный счёт»:

это ключевая фраза в арсенале мошенников.

Мошенники предлагают своим жертвам то, чего им не предлагают банки!

#morphologicalanalysis
#NLP=anchor
#customersRoutsideofBank'sSecurityPerimeter
#marketwantssecureaccounts
#cottonclub
#brandiscreated
#jimmy #picklock

Фрод[exists] является доказательством наличия НЕУДОВЛЕТВОРЁННОГО спроса на защищённые / безопасные счета.

Клиенты хотят большей защищённости.

Неудовлетворенный спрос - нереализованная ввиду отсутствия нужных товаров или несоответствия их ассортимента и качества требованиям покупателей часть действительного **спроса**.

cyberleninka.ru

Спрос и его роль в категориях потребности и потребления – тема научной…

#какповыситьбоевуюустойчивостьклиентов

Закон Парето для банков:

- 20% усилий дают 80% результата;
- 20% меню дают 80% выручки;
- 20% клиентов дают 80% депозитов / дохода;
- … и эти 20% хотят бо̲льшей информационной безопасности!

#showMEtheMONEY
#how2useFRAUD=slipstream


Google
NXP
gemalto
security to be free
PayPal
SAMSUNG
Daon
QUALCOMM
Alibaba Group
amazon
Lenovo
BCcard
Infineon
RSA
fido
TM
yubico
Trust the Net
egis
AMERICAN EXPRESS
intel
nok nok
ALLIANCE
ING
Synaptics
IDEMIA
augmented identity
FEITIAN
WE BUILD SECURITY
ARM
aetna
Bank of America
Microsoft
docomo
VISA
RAON
SECURE
dedicated to changing the way online authentication is done.


Цена - $ 25..50...950 USD
Penetration <= 0.05%

Золотое правило ИБ от Engine.ER Lab:

- НЕ СТОЙ под стрелой !
- НЕ РАБОТАЙ под напряжением!
- НЕ ДЕРЖИ зарегистрированную SIM-карту в смартфоне!

1

Как защититься от хакеров?
Переставьте SIM-карту из смартфона в кнопочный телефон!
SMS с кодами подтверждения будут "приземляться" на кнопочный телефон.

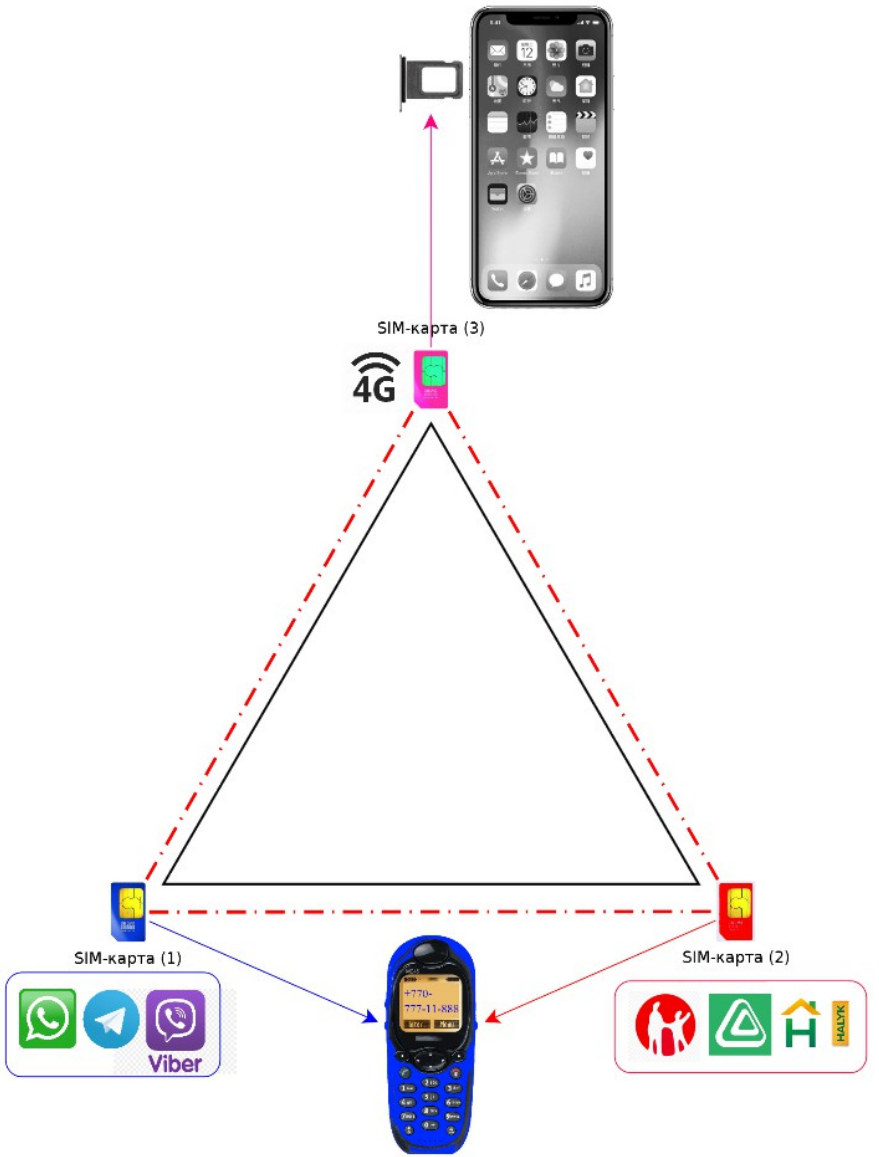
Хакеры не могут прочитать SMS с кодами подтверждения с кнопочного телефона.
Поэтому они не смогут украсть Ваши деньги и аккаунты в мессенжерах и социальных сетях, даже если взломают Ваш смартфон. А в смартфон надо просто установить новую SIM-карту с другим номером. Приложения в Вашем смартфоне не заметят изменений и будут работать как прежде.

Схема #coldstoragephone

#coldstoragephone=User'sZeroTrustSolution

#whyWErunSMSauthentication
#watchdog
#CSMA - Cybersecurity Mesh Architecture

- #SMSinterception
- #unauthorized use
- #SIMswapping #userOUTofControl



Первый треугольник Кана

КАК настроить: coldstoragephone
#coldstoragephone на dzen.ru

#rigidityTriangle
#hacker resistant phone
#GSMpenetration

Beeline : *102# или *160#

Tele2 : *111# или *120#

Kcell : *111# или *114#

Altel : *111# или *127*2#

1

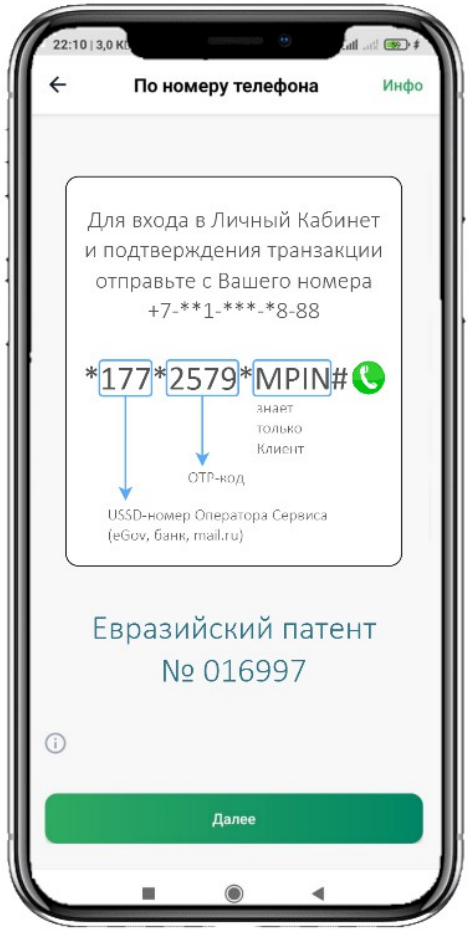
Как защититься от хакеров?
Переставьте SIM-карту из смартфона в кнопочный телефон!
SMS с кодами подтверждения будут "приземляться" на кнопочный телефон.

Хакеры не могут прочитать SMS с кодами подтверждения с кнопочного телефона.
Поэтому они не смогут украсть Ваши деньги и аккаунты в мессенжерах и социальных сетях, даже если взломают Ваш смартфон. А в смартфон надо просто установить новую SIM-карту с другим номером. Приложения в Вашем смартфоне не заметят изменений и будут работать как прежде.

Схема #coldstoragephone

2

IM-Token 2FA +++++ :
заменяем OTP-via-SMS на USSD-Up



- #killphishermode - фишинг исключен КАК КЛАСС;
отправить USSD без SIM-карты невозможно;
- защита от незаконного перевыпуска SIM-карты;
- защита от несанкционированного использования;
- исключаем риск перехвата валидного SMS-кода.

#killphishermode
#GSM=VPN(SIM-tokens)
#IPC.KG=Pilot(SMS-ATM)
#можетлибанкгарантировать
#бумажнаябезопасностьVSинженерная защита
#emergence

1

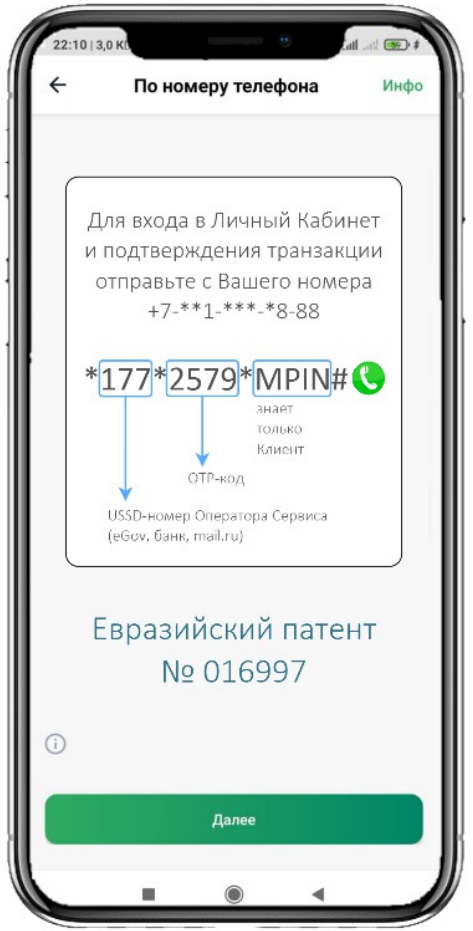
Как защититься от хакеров?
Переставьте SIM-карту из смартфона в кнопочный телефон!
SMS с кодами подтверждения будут "приземляться" на кнопочный телефон.

Хакеры не могут прочитать SMS с кодами подтверждения с кнопочного телефона.
Поэтому они не смогут украсть Ваши деньги и аккаунты в мессенжерах и социальных сетях, даже если взломают Ваш смартфон. А в смартфон надо просто установить новую SIM-карту с другим номером. Приложения в Вашем смартфоне не заметят изменений и будут работать как прежде.

Схема #coldstoragephone

2

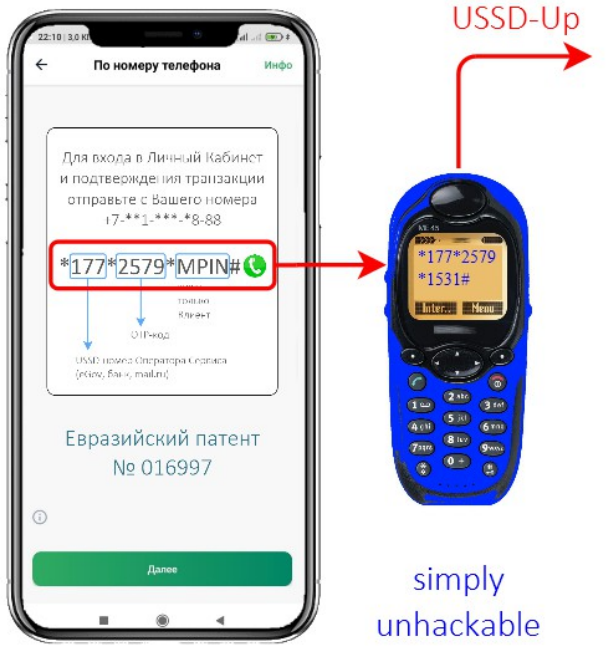
IM-Token 2FA +++++ :
заменяем OTP-via-SMS на USSD-Up



- #killphishermode - фишинг исключен КАК КЛАСС; отправить USSD без SIM-карты невозможно;
- защита от незаконного перевыпуска SIM-карты;
- защита от несанкционированного использования;
- исключаем риск перехвата валидного SMS-кода.

3

IM-Token 2FA +++++ Highest Security:
(режим максимальной безопасности).



simply unhackable

- удалённое управление кнопочным телефоном невозможно;
- компрометация смартфона / web-терминала не приводит к компрометации токена (SIM-карты) и секрета (MPIN);
- SIM-карта изолирована от сети Интернет аппаратным межсетевым экраном / firewall (соответствует концепции Cybersecurity Mesh Architecture - CSMA);
- улучшает usability - не нужно регулярно менять пароли.


4:40
17:31
10:32


5200
mAh


VERTU


10:45
ELARI
CardPhone


20:16

10:44, 1 августа 2021 Наука и техника

Названа доля пользующихся кнопочными телефонами россиян

Доля пользующихся кнопочными телефонами абонентов «ВымпелКома» (является брендом «Билайн») составляет около 23 процентов. Об сообщает РБК со ссылкой на аналитические отчеты компании.

Nokia 3310. Фото: Максим Блинов / РИА Новости

С чего начать:

- аутентификация сотрудников банка / министерств в корпоративной сети (EMPs authentication);
- мобильный банкинг для юридических лиц (ЮЛ) (#coldstoragephone в сейфе);
- надёжный 2FA+ для (облачных) ЭЦП;
- «чужие»* 20% клиентов, которые дают 80% дохода;
- Suńqar Alliance — защищённые бесплатные переводы.

* - клиенты других банков

Как банкам заработать деньги на фроде?

Займите незанятую господствующую высоту
#самыйзащищённыйбанк / #безопасныесчета
и ждите клиентов, которые сами придут в банк под давлением фрода.

#how^to ride^the fraud
#jacktrout — flanking
#callmethemostsecuritybank
#notOnlySuperApps
#казахстанскийфондгарантированиядепозитов
#where2goClustomerAfterIncidents?

В Kaspi сообщили об устранении сбоя и объявили о "подарке" за моральные издержки

28 октября 2020 15:54 | Рубрика: Общество

Компания призвала не доверять фейковым рассылкам и предоставила своим клиентам бонус в качестве компенсации за причиненные неудобства.

Восстановлена работа сервисов приложения Kaspi.kz, передает Arnapress.kz.

Сравнительная таблица:

	OTP-via-SMS	IM-Token 2FA+++++	FIDO **U2F**
Токен	SIM-карта	SIM-карта	USB-токен с аппаратной кнопкой
Стоимость токена	0	0	$ 30...1000 USD
Есть аппаратная кнопка для проверки физического присутствия пользователя (physical 'test of user presence')	Нет	Да*	Да
Аутентификация возможна только при физическом наличии SIM-карты / токена	Нет, возможен перехват SMS	Да	Да
Используемый сервис сети GSM	SMS-Down ↓	USSD-Up ↑	-
Режим работы мобильного телефона клиента	Приёмник ↓	Передатчик ↑	-
Канал Аутентификации	Интернет**	GSM	Интернет
Канал Аутентификации изолирован от сети Интернет	Нет	Да	Нет
▲Токен изолирован от сети Интернет аппаратным firewall	Нет**	Да*	Нет
▲Способ защищён от несанкционированного перевыпуска SIM-карты (SIM-swapping)	Нет	Да, с помощью hash ICC-ID	Да
Защита от несанкционированного использования	Нет	Да, с помощью MPIN	Нет***
▲Способ защищён при компрометации endpoint Web-терминала (смартфона / ПК / планшета)	Нет	Да*	Да
Способ защищён от перехвата валидного OTP-кода	Нет	Да	-
Способ защищён от фишинга (phishing)	Нет	Да	Да
Native Usability / Driver's Free	Да	Да	Требуется настройка

* - при использовании #coldstoragephone

** - ввод OTP-кода (*секрета*) и аутентификация осуществляется через web-терминал и сеть Интернет. GSM используется только для доставки OTP-кода клиенту.

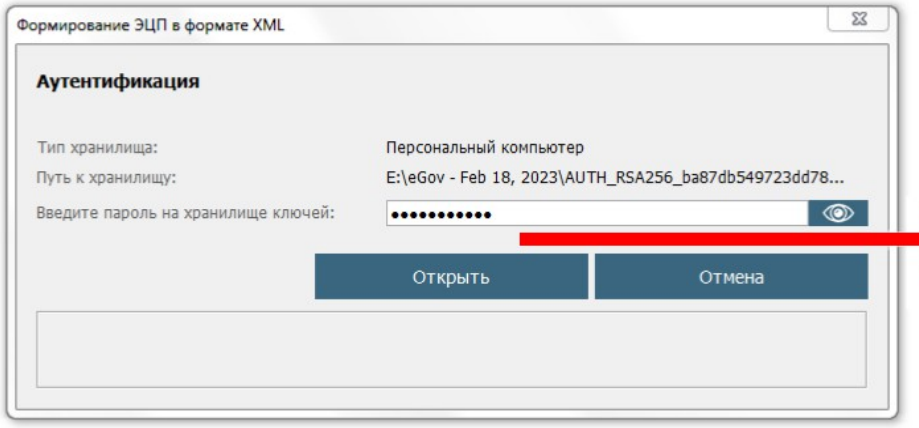
*** - кроме U2F токенов со считывателем fingerprint;

egov 1414 Зарегистрироваться RU

Вход на портал

Логин/пароль | ЭЦП | Digital-ID | QR-код

Выбрать сертификат



Аутентификация

Отправьте с Вашего зарегистрированного в БМГ номера мобильного телефона +7-7*7-***-18-88

*1414*7108*MPIN#

Чем я могу Вам помочь?

14:01, 14 ноября 2022

Интернет-мошенники обманули казахстанцев на 15 млрд тенге

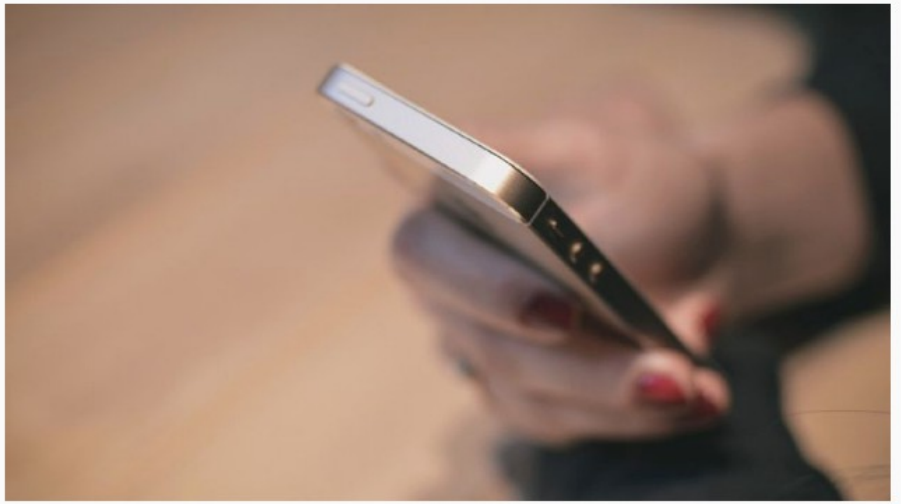


Фото: pixabay

Заместитель начальника Центра по борьбе с киберпреступностью МВД Рустем Дюсетаев рассказал 14 ноября, какие виды мошенничества преобладают в Казахстане, передает корреспондент Zakon.kz.

Рустем Дюсетаев заявил, что в стране участились случаи совершения киберпреступлений, в том числе мошенничеств в отношении интернет-пользователей.

zakon.kz

12:16, 24 апреля 2023

Ущерб от интернет-мошенников составил 3 млрд тенге с начала года

Фото: freepik

Начальник центра по борьбе с киберпреступностью департамента криминальной полиции МВД РК Жандос Суюнбай на традиционном брифинге ведомства рассказал, сколько денег казахстанцы потеряли от действий интернет-мошенников в этом году, сообщает корреспондент Zakon.kz.

Представитель ведомства добавил, что в период с 18 по 20 апреля 2023 года на территории страны проведено оперативно-профилактическое мероприятие "Anti-fraud", направленное на повышение эффективности мер по борьбе с правонарушениями, совершаемыми с использованием информационных технологий.

За 2022 год интернет-мошенники обманули казахстанцев на 15 млрд тенге.

КАПИТАЛ
ЦЕНТР ДЕЛОВОЙ ИНФОРМАЦИИ

Казахстанцы чаще всего сталкиваются с телефонным и интернет-мошенничеством

Основная группа риска - люди пенсионного возраста

09.03.2023

09.03.2023 · 14:46

Большая часть казахстанцев сталкивалась с финансовым мошенничеством – таковы результаты социологического исследования, проведенного Агентством по регулированию и развитию финансового рынка в 2022 году. Подробнее о распространенных схемах обмана и способах защиты от мошенников **центру деловой информации Kapital.kz** рассказал директор Департамента защиты прав потребителей финансовых услуг АРРФР Александр Терентьев.

Согласно социсследованию, **55,8%** респондентов сталкивались с финансовым мошенничеством, из них **34,2%** – с телефонным мошенничеством (вишинг), **32,7%** – с интернет-мошенничеством (фишинг). **21,6%** опрошенных были участниками мошенничества со стороны финансовых пирамид, **11,5%** – с платежными картами.

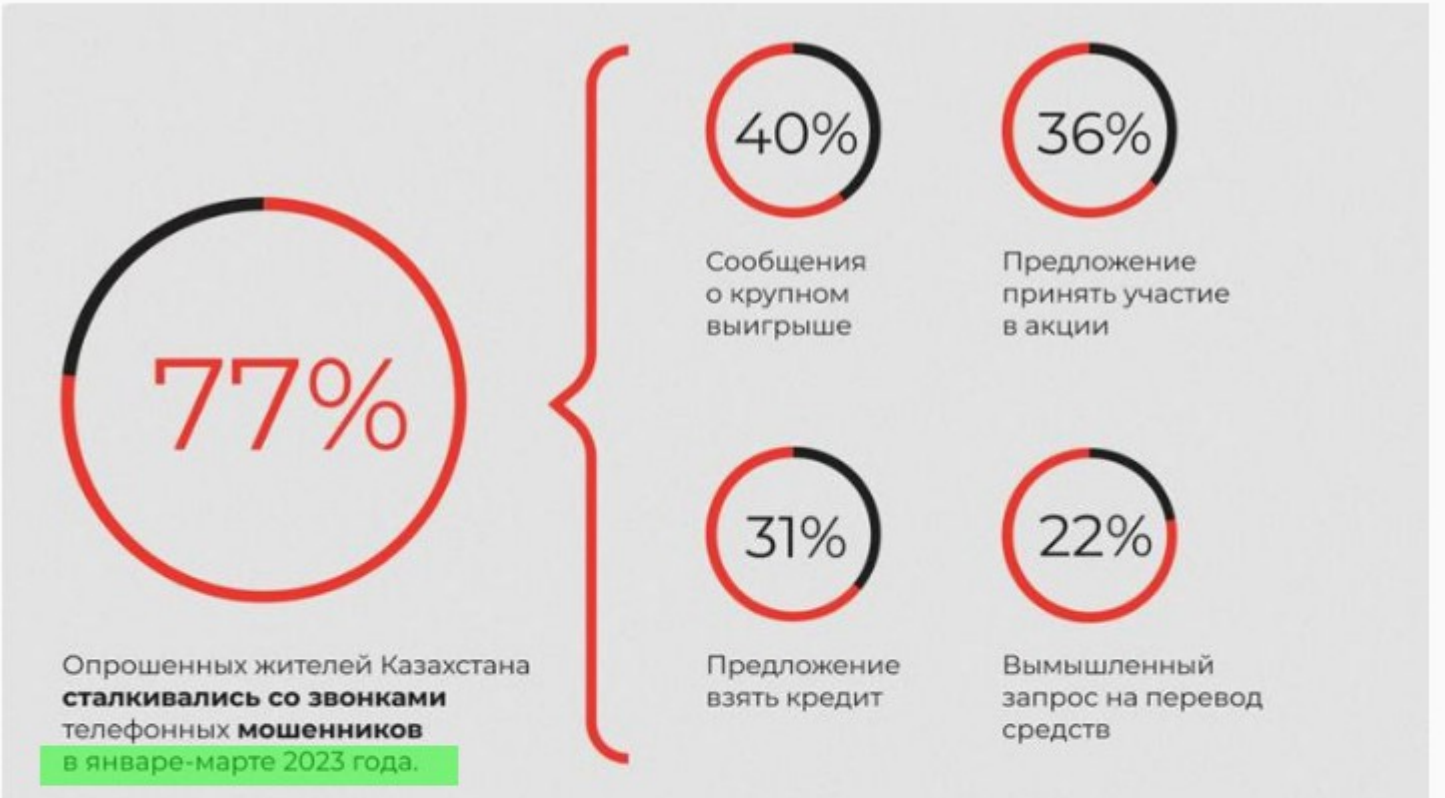


Фото: Aquarelle Research

zakon.kz 18 Мая 2023

77% опрошенных заявили, что действительно сталкивались со звонками телефонных мошенников. При этом 18% респондентов отметили, что частота таких звонков увеличилась.

Engine.ER

Сбер посчитал, сколько кредитных миллиардов россияне за год пытались отдать мошенникам

ЛЕНТА НОВОСТЕЙ | 03.03.2023 15:18 | 5 646 | Время прочтения: 1 минута

АВТОР

Анелия Каткова

автор новостного контента Банки.ру

ИСТОЧНИК

«Прайм»

ТЕМЫ

Сбербанк

В 2022 году россияне пытались взять кредиты на общую сумму 200 млрд рублей под воздействием мошенников, которые затем собирались похитить эти средства, пишет «Прайм» со ссылкой на презентацию начальника управления противодействия кибермошенничеству Сбербанка Сергея Велигодского.

«Двести миллиардов рублей пытались украсть кредитных денег у наших граждан», — рассказал Велигодский. По его данным, это «общая сумма кредитов, которую граждане РФ пытались оформить под воздействием мошенников за 2022 год». Из представленных Сбером материалов следует, что всего четверть хищений путем телефонного мошенничества «совершается с использованием кредитных средств».

По данным банка, в прошлом году 83% граждан столкнулись с попыткой кибермошенничества. Всего было зафиксировано 5 млрд попыток телефонного мошенничества.

Общий ущерб клиентов банков от кибермошенников в 2022 году составил 14 млрд рублей, напомнил Велигодский. «Важно отметить, что это не все потери, потому что есть еще статистика МВД… нет официальных цифр, но неофициальные — там порядка 100 миллиардов рублей мы сегодня знаем», — добавил топ Сбера. По его словам, это следует из заявлений граждан о хищении денег путем дистанционного мошенничества.

30 ноября 2015 г.

Фрод-инциденты на 80% произрастают изнутри компаний

Согласно исследованиям аналитической фирмы Kroll, фрод-инциденты (подлог или злонамеренное использование данных, от англ. fraud — мошенничество) в 2014 г. произошли в 75% компаний, что соответствует росту на 14% за три года. В 81% из них за этими инцидентами стояли их собственные служащие, тогда как в предыдущем исследовании этот показатель составлял 72%. При этом обращение в компетентные органы по поводу фрод-инцидентов были поданы только в 41% случаев.

Финансовые потери в результате фрода в 2014 г. понесли 69% компаний, тогда как ранее этот показатель составлял 64%. Наиболее часто — в 22% случаев — в результате фрода происходит воровство физических активов, 17% инцидентов приходится на фрод в области производства, поставок или приобретение оборудования, а на кражу информации — 15%.

По данным аналитиков, количество мошеннических инцидентов выросло за последние три года на 14%. При этом в 2014 г. 81% преступлений совершались мошенниками одиночками, тогда как в предыдущий год этот показатель составлял 72%.

Исследование показало, что подлогу от рук собственных менеджеров компании старшего или среднего звена подвергалась одна из трех жертв (36%), молодые сотрудника были замечены в мошенничестве в 45% случаев, а 23% преступлений совершались агентами компании или посредниками.

В компаниях, где за последние 12 месяцев были зафиксированы кража или атаки на данные, в 45% случаях типовыми виновниками инцидентов были сотрудники компаний-жертв, а в 29 случаях за инцидентом стояли производитель и поставщик услуг. Лишь ничтожный процент пришелся на инциденты от внешних атак или хакеров на саму компанию — всего 2%, а на поставщика услуг или производителя — 7%.

LENTA.RU

10:25, 25 апреля 2023

Двое профессоров российских вузов отдали мошенникам восемь миллионов рублей

Телефонные мошенники обманом похитили у двух профессоров российских вузов 8,5 млн рублей

Фото: Алексей Сухоруков / РИА Новости

Двое профессоров российских вузов поверили представлявшимся сотрудниками Центробанка телефонным мошенникам и перевели им свои сбережения. Об этом сообщает Telegram-канал Mash.

Пострадавшие — преподаватели МГУ и МГТУ 63 и 85 лет. Им позвонили аферисты и запугали тем, что у них крадут средства на банковских счетах. Профессорам предложили спасти сбережения, отправив переводом на «безопасные счета». Потерпевшие выполнили указания: один перевел мошенникам семь миллионов рублей, второй — полтора миллиона рублей.

Россиянам рассказали о новом способе мошенничества с банковскими картами

Начальник управления противодействия кибермошенничеству Сбербанка Сергей Велигодский в рамках форума AntiFraud Russia рассказал россиянам о новом способе кражи денег с банковских карт. Его слова приводит РИА Новости.

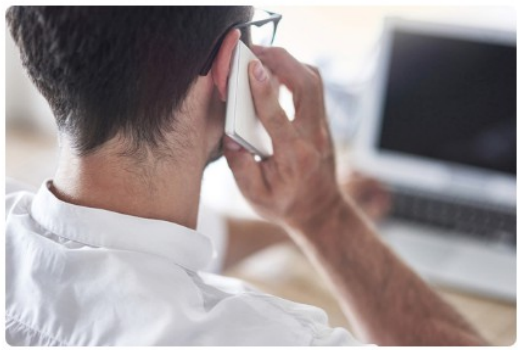


Фото: Westend61 RF / gpointstudio /

Злоумышленники рассказывают жертве о «новой защищенной карте», которую следует привязать к смартфону и перевести на нее средства. Когда человек выполняет их указания, деньги с карты обналичиваются через банкомат, поскольку физически она находится у мошенников.

Еще одна схема задействует банковские кредиты. Жертве рассказывают о якобы выданном потребительском займе, для отмены которого необходимо подать заявку на новый и перевести средства на некий «защищенный счет».

05:31, 8 октября 2021 Экономика

Раскрыты любимые слова телефонных мошенников

DeviceLock: мошенников распознают по словосочетаниям «лицевой счет» и «финансовая ячейка»

Фото: Pixabay

Телефонных мошенников можно распознать по их любимым словосочетаниям «лицевой счет» и «финансовая ячейка», раскрыли эксперты в исследовании компании-производителя систем борьбы с утечками данных DeviceLock. Содержание публикует РИА Новости.

Как выяснили авторы исследования, мошенники постепенно уходят от использования банковских баз данных, которые подорожали из-за мер борьбы с утечками, и чаще выманивают информацию о счетах в банке.

По словам директора компании DeviceLock DLP Юрия Томашко, злоумышленники используют легенду о том, что на имя жертвы якобы взят кредит с использованием лицевого счета, который привязан к паспортным данным. Для предотвращения хищения потенциальной жертве необходимо назвать номера ее банковских счетов и перевести все средства на некий безопасный счет. При этом жертву просят не говорить никому о звонке, поскольку это якобы нарушает Уголовный кодекс.

ГОРОД / 04:21, 25 апреля 2023 1 мин. – а А +

Раскрыта новая схема мошенничества с переводом денег в цифровые рубли

Мошенники начали предлагать пенсионерам переводить накопления в цифровые рубли.

Телефонные мошенники под видом сотрудников пенсионного фонда начали звонить пожилым людям и предлагать переводить накопления на платформу цифрового рубля. Злоумышленники обещают своим жертвам разовую выплату в десять процентов от суммы сбережений, перечисленных на якобы защищенный счет Центробанка в цифровых рублях, и ежемесячную прибавку к пенсии в том же размере в течение года.

21 февраля 2023, 10:54 2137

Уральский форум «Кибербезопасность в финансах». Итоги. Тренды. Ожидания

14–17 февраля 2023 года в Екатеринбурге прошел Уральский форум «Кибербезопасность в финансах». В дискуссии приняли участие представители Банка России, федеральных органов власти, банков и небанковских финансовых организаций, финтех-структур и, конечно же, эксперты ведущих компаний в области защиты информации. Журнал «ПЛАС», выступивший информационным партнером Уральского форума, резюмирует ключевые итоги мероприятия.

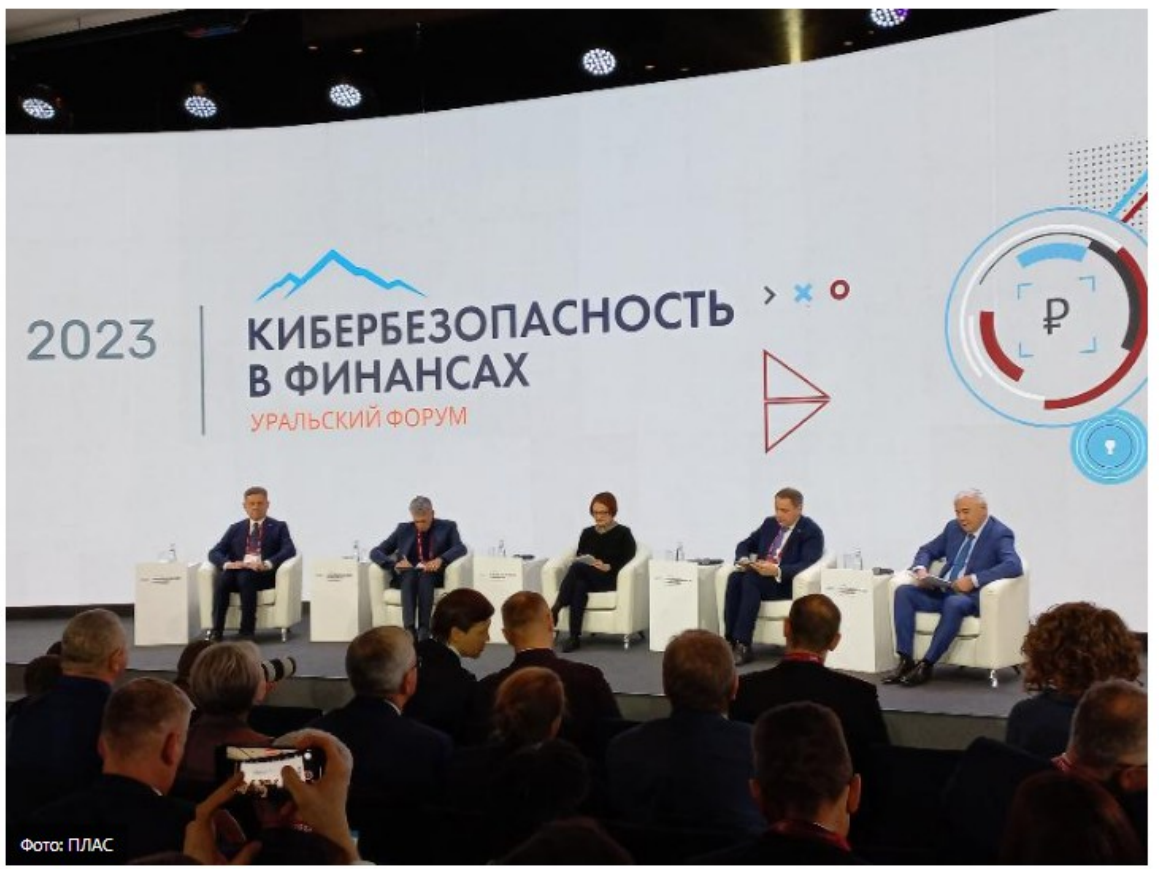


Фото: ПЛАС

Как отметил **Александр Егоркин**, первый вице-президент Банка Газпромбанка, 90% фрода сегодня приходится на телефонное мошенничество.

В то же время, по словам **Сергея Хренова**, директора департамента предотвращения мошенничества и потерь доходов «МегаФон», за прошедший год ситуация с телефонным мошенничеством значительно улучшилась, к концу 2022 года поднявшаяся волна звонков с подменных номеров была сбита.

Основной преступный тренд сегодня – подмена номеров зарубежных операторов с попыткой выдать их за мобильные российские. Зачастую такую ситуацию трудно выявить, поскольку подменный номер может напоминать российский номер в роуминге.

Однако это в основном проблема малых операторов, поскольку крупные российские операторы уже создали общий верифицированный контур, с помощью которого успешно противостоят мошенникам. Так, Мегафон сегодня блокирует 7–10 млн таких звонков в неделю.

По данным Банка России, объем операций без согласия клиента в 2022 году вырос на 4% по сравнению с 2021 годом и достиг 14 млрд рублей. При этом каждая вторая мошенническая операция пришлась на социальную инженерию.

На этом фоне Банк России планирует принять широкий комплекс мер по защите потребителя, включая персональную ответственность банковских менеджеров за потери населения от фрода.

По словам **Германа Зубарева**, заместителя председателя Банка России, основными направлениями деятельности регулятора в области ИБ на ближайший трехлетний период являются:

- защита потребителей и повышение их доверия к кредитно-финансовым структурам;
- достижение технологического суверенитета;
- управление киберрисками и контроль операционной надежности.

Gartner Research

The Future of Security Architecture: Cybersecurity Mesh Architecture (CSMA)

Published: 12 January 2022

Summary

CSMA is an emerging approach for architecting composable, distributed security controls to improve your overall security effectiveness. Security and risk management technical professionals can use this blueprint to start aligning their roadmap for security and IAM technologies that plug into a mesh.

Included in Full Research

Gartner 2022 security trend #7: Cybersecurity Mesh

Dec. 16, 2022 | Tony Burgess

This is the seventh and final entry in our series of articles about the seven key trends identified in Gartner's report "Top Trends in Cybersecurity 2022," released to its clients last March. The final trend to be discussed is "Cybersecurity Mesh."

This trend refers to the emergence of a new category of solutions and services that Gartner calls a cybersecurity mesh architecture (CSMA). In a remarkable statement of how important they consider this trend, Gartner predicts that in just over a year, the adoption of CSMA will enable organizations to reduce the financial impact of any given security incident by 90% on average.

That's a big impact.

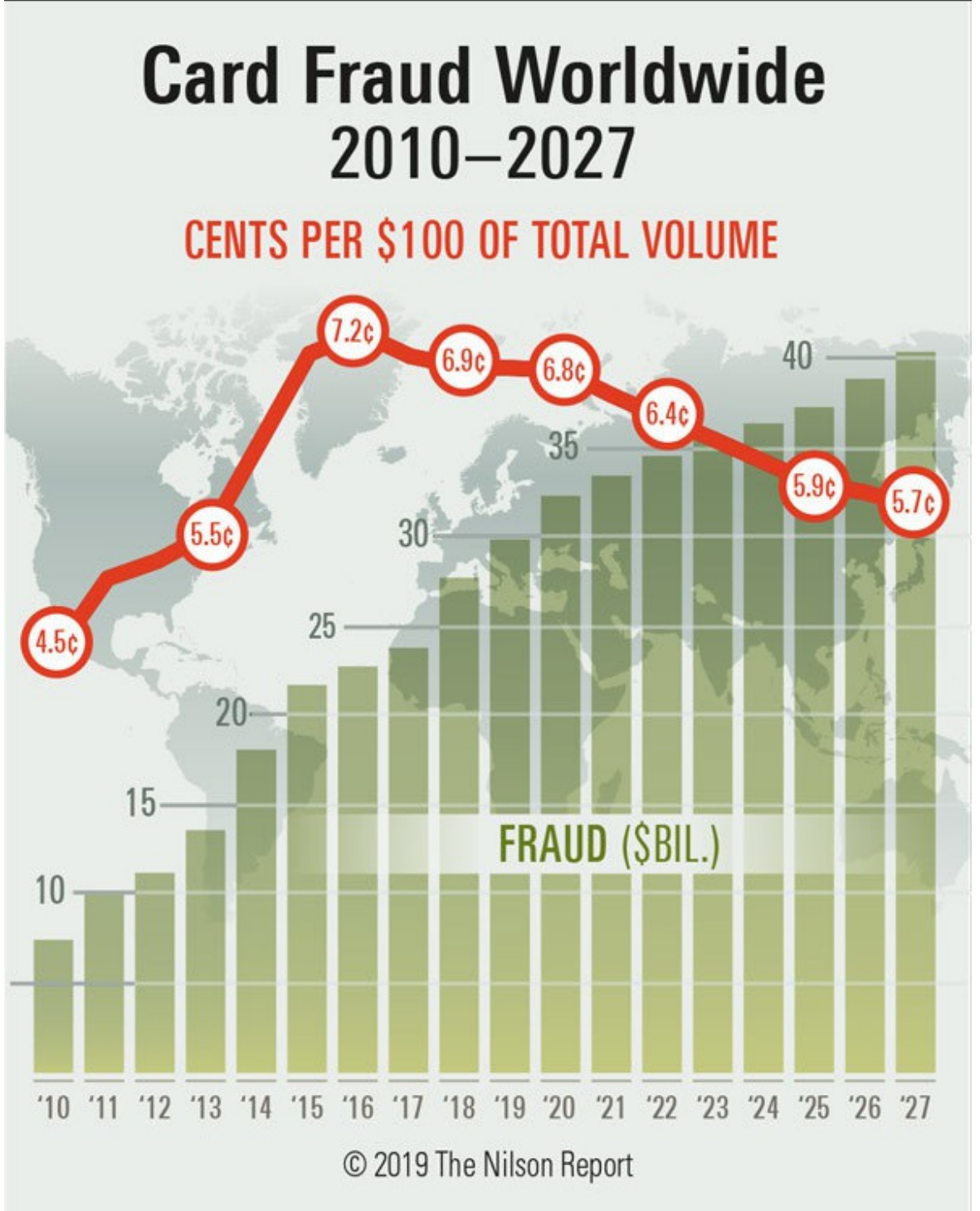
Новости

Cybersecurity mesh – управление защитой данных на локальном уровне

22.02.2021

Cybersecurity mesh («сеть кибербезопасности») – метод защиты, который подразумевает переход от глобальных мер к частным. Вместо построения единого цифрового периметра вокруг всех устройств или узлов ИТ-сети, специалисты по кибербезопасности советуют защищать каждую точку отдельно.

Согласно данным компании Gartner, новые меры по защите данных будут активно внедрять в 2021 году. Переход от общего к частному вполне закономерный. В связи с распространением цифровых технологий, а также доступностью IoT-устройств, хакеры находят все больше их уязвимостей. К примеру, в случае с «интернетом вещей» это приводит к созданию ботнетов для целенаправленных кибератак. В отчете Check Point за 2020 год сказано, что всего за год количество подобных атак увеличилось примерно на половину. Это значит, что нужно использовать более эффективные методы защиты, и cybersecurity mesh – один из них.


Card Fraud Worldwide
2010–2027
CENTS PER $100 OF TOTAL VOLUME
4.5¢
5.5¢
7.2¢
6.9¢
6.8¢
6.4¢
5.9¢
5.7¢
FRAUD ($BIL.)
10
15
20
25
30
35
40
'10 '11 '12 '13 '14 '15 '16 '17 '18 '19 '20 '21 '22 '23 '24 '25 '26 '27
© 2019 The Nilson Report

Согласно [прогнозам Gartner] (https://www.gartner.com/en/articles/the-top-8-cybersecurity-predictions-for-2021-2022-1),

> ***«К 2024 году организации, использующие CSMA, снизят финансовые последствия инцидентов безопасности в среднем на 90 %».***

Практичная ячеистая архитектура кибербезопасности потребует более сильного, консолидированного управления политиками и руководства. Например, очень важно разработать более подходящие политики доступа с минимальными привилегиями, которых организации могут добиться, **используя механизм централизованного управления политиками с распределенным применением**.

Тем не менее, нам все еще нужен клей, чтобы склеить все доступные инструменты. К счастью, благодаря рекомендациям, содержащимся в отчете Gartner CSMA, становится возможной интеграция с распространенными языками кибербезопасности — API и открытыми стандартами, а также тщательно задействуется весь существующий стек безопасности.

Спасибо за чтение. Да пребудет с вами информационная безопасность□.

20:08, 10 мая 2018 Экономика

Найдено секретное хранилище биткоинов с миллиардами долларов

Порядка семи процентов всех добытых в мире биткоинов хранятся на серверах компании Харо, размещенных в охраняемом бывшем военном бункере в горах Швейцарии. Стоимость такого объема криптовалюты оценивается в 10 миллиардов долларов, сообщает Bloomberg со ссылкой на источники.

Фото: Rick Bowmer / AP

«Это значит, что всего за четыре года (Харо начала предоставлять услуги по хранению в 2014 году — *прим. «Ленты.ру»*) размер депозитов Харо превысил суммы, которые находятся на счетах 98 процентов от порядка 5670 банков США», — пишет Bloomberg.

Бункер представляет собой так называемое холодное хранилище биткоинов — в нем криптовалюта хранится в режиме офлайн, что сводит к минимуму угрозу кражи. Чтобы получить свои биткоины из такого хранилища, у клиентов Харо уходит около двух дней — в это время компания проверяет личность клиента и подлинность его запроса на перевод криптовалюты. Затем Харо вручную подписывает транзакции приватными ключами, находящимися в разных локациях бункера.