



Управление по противодействию
киберпреступности

Основные способы совершения киберпреступлений

Витебск, 2024

Статистика

Имущественный вред, причиненный киберпреступлениями в 2023 году гражданам жителям Витебской области составил более 2,5 млн рублей.

80% преступлений совершается в отношении городских жителей.

Самым пожилым по 86 лет, из Витебского района и Витебска, они установили программное обеспечение

В 2023 году пострадали не менее 91 работника государственных учреждений образования, из них 76 причинен материальный ущерб.

Средний возраст 44 года

Киберпреступления оставили 19% от всех зарегистрированных областива 2023 год.

ПОРТРЕТ жертвы киберпреступника

женщины - 60%;

в возрасте от 18 до 60 лет - 81%;

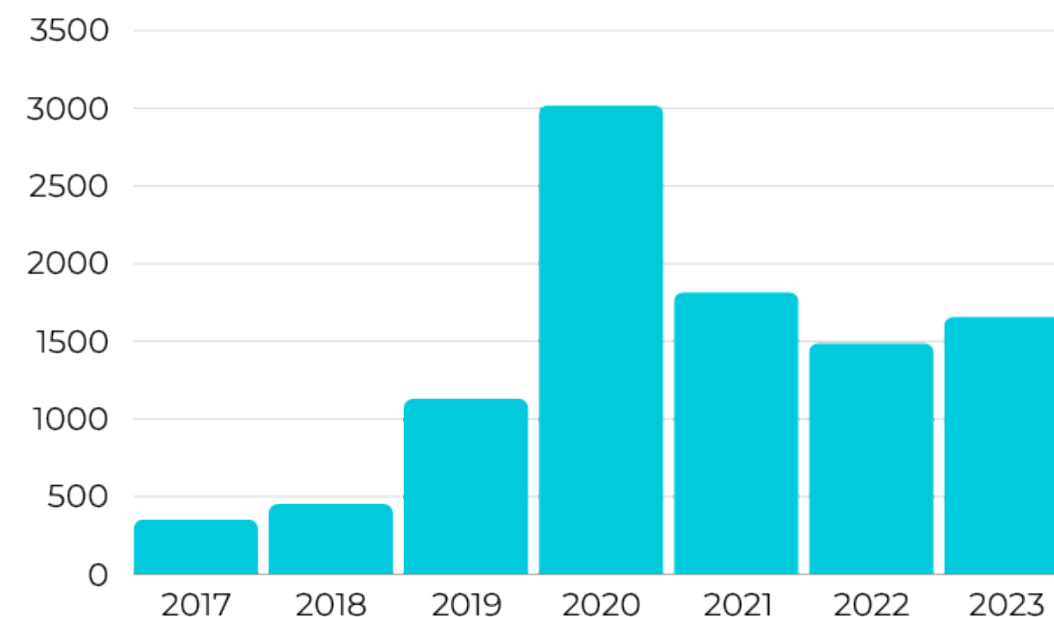
с высшим образованием - 41%;

со средним уровнем дохода;

имеющая постоянную работу;

В 2024 году уже пострадали более 400 граждан (около 40 человек еженедельно).

Максимальный ущерб у одного потерпевшего составил более 97 тысяч рублей. Женщина перевела переводила деньги за посылку от мужчины с сайта знакомств.



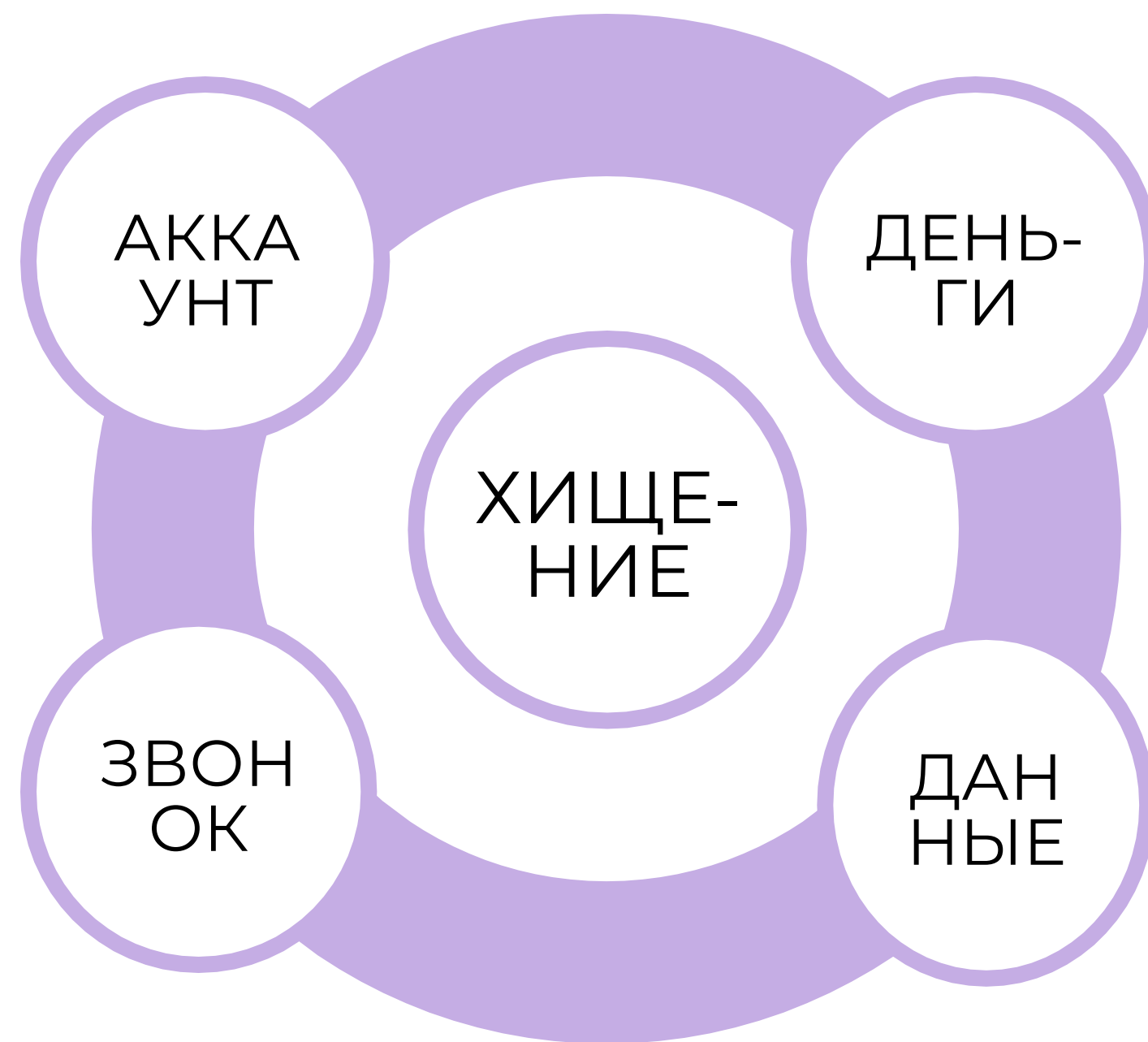
Мошенничества и хищения имущества составляют более 80% от всех киберпреступлений

Доступ к аккаунту

Владельцы сами предоставляют доступ к своим аккаунтам, после чего с их учетной записи **рассылаются сообщения** с просьбой денег в долг или оказать помощь больному человеку.

Звонок в мессенджере

Мошенники представляются сотрудниками правоохранительных органов, банковских организаций, родственниками, знакомыми. Могут убедить установить программное обеспечение, получить кредит, перевести деньги на «защищенный счет».



Сообщение в соцсетях или мессенджере

Используя искусственный интеллект мошенники создают голосовые сообщения с просьбой перевести деньги или создают фейковые магазины

Получение персональных данных

ФИШИНГ поддельные сайты банковских организаций или криптобирж.

Получив личные данные, похищают деньги или открывают счета и проводят похищенные деньги



Telegram-канал "Цифровая грамотность"
@cifgram

Фейковый конкурс рисунков по ссылке “друга”

Онлайн-конкурс детского рисунка "ВОЛШЕБИЦА ЗИМА" 1/4 финала.

На конкурс принимаются к участию работы в жанрах: пейзаж, натюрморт.

Даты проведения конкурса: 1 февраля 2024 года по 26 февраля 2024 года.

Дата подведения итогов: до 1 марта 2024 года.

Претендент №1 - Ксения Артемьева (11 лет)

👍👍👍 ПРОГОЛОСОВАТЬ ЗА КСЮШУ 👍👍👍



Претендент №4 - Александра Фролова (10 лет)

👍👍👍 ПРОГОЛОСОВАТЬ ЗА САШУ 👍👍👍



Претендент №6 - Николай Ручкин (8 лет)

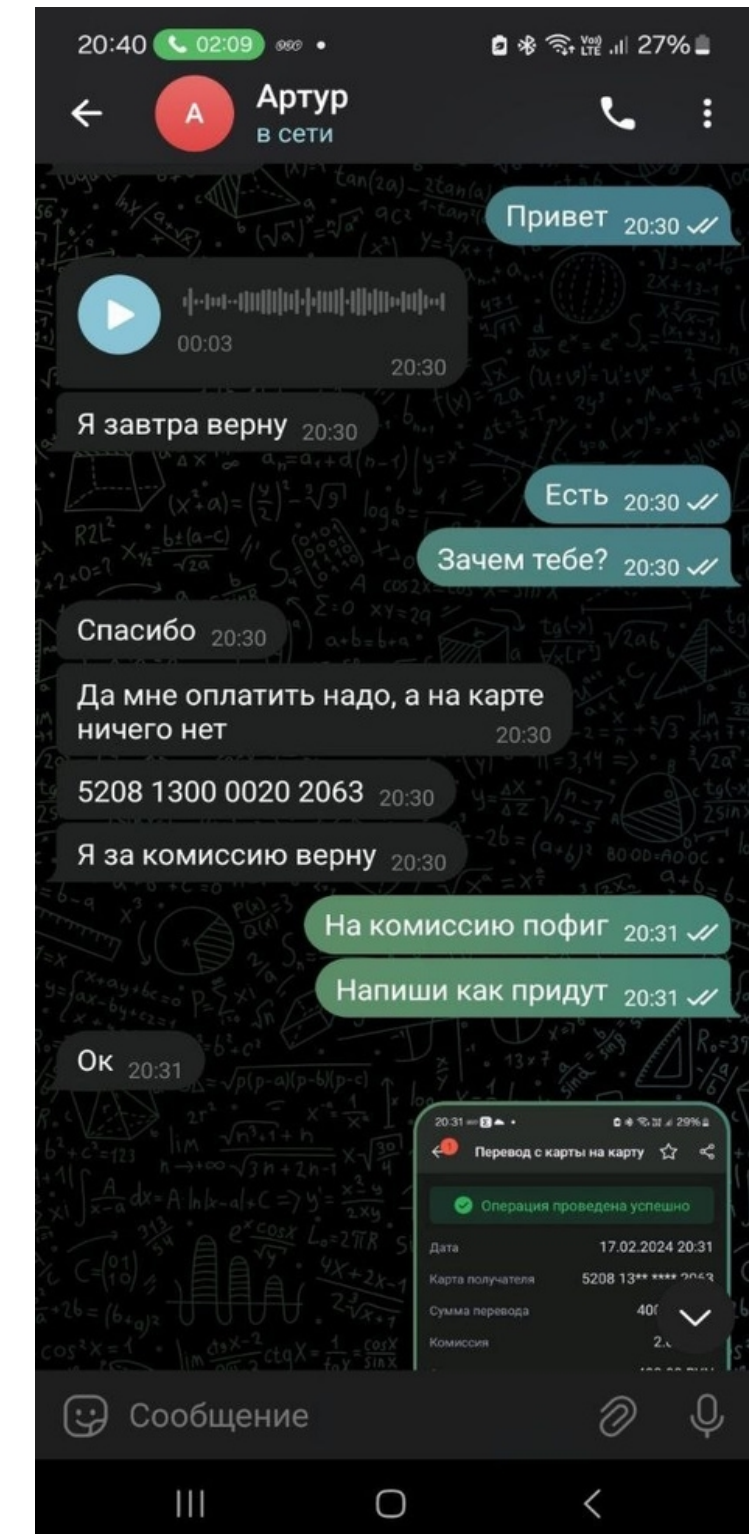
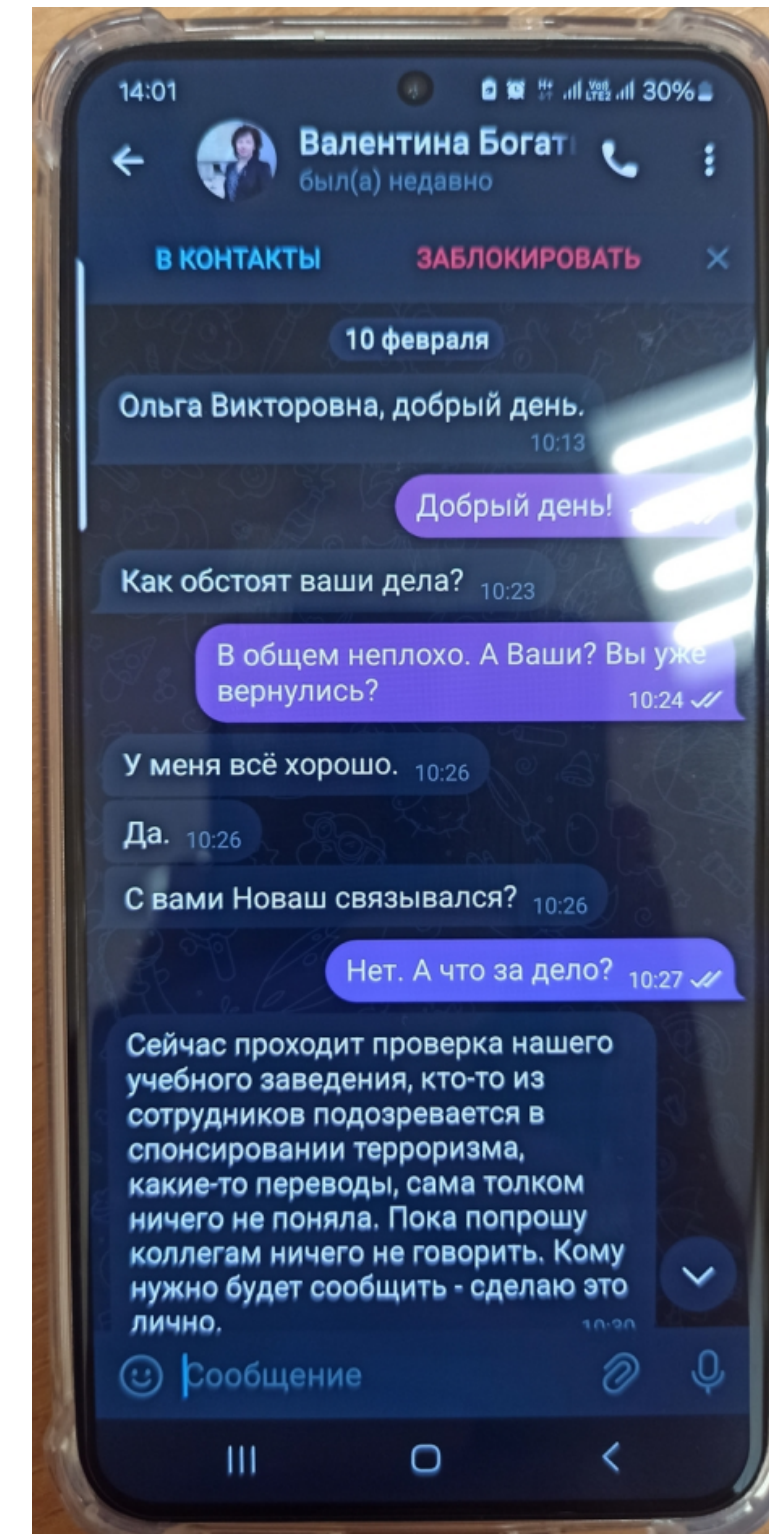
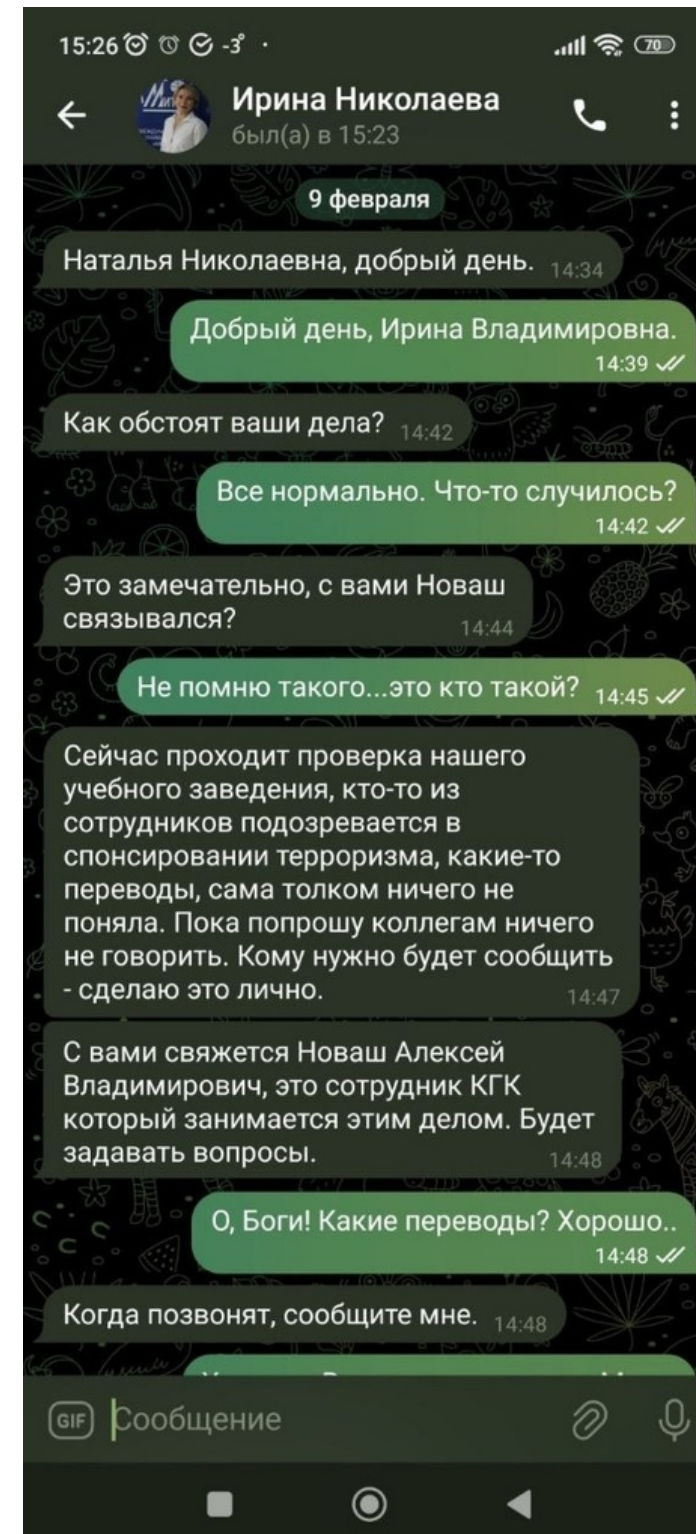
👍👍 ПРОГОЛОСОВАТЬ ЗА КОЛЮ 👍👍👍



СУТЬ схемы

Рисунки созданы нейросетью. Мошенники получают доступ к аккаунту и рассылают контактам абонента сообщения с просьбой проголосовать за сына или дочь. Для подтверждения голоса требуется подтвердить свой номер телефона и поступивший код из сообщения. Полученный новый аккаунт используется для продолжения рассылки, в том числе сообщений о помощи больным детям.

Создают новый аккаунт и текстовые (голосовые) сообщения от имени знакомых для побуждения к выполнению действий другого мошенника, который может представиться сотрудником госорганов (1-3). Или голосом друга попросить денег (4).



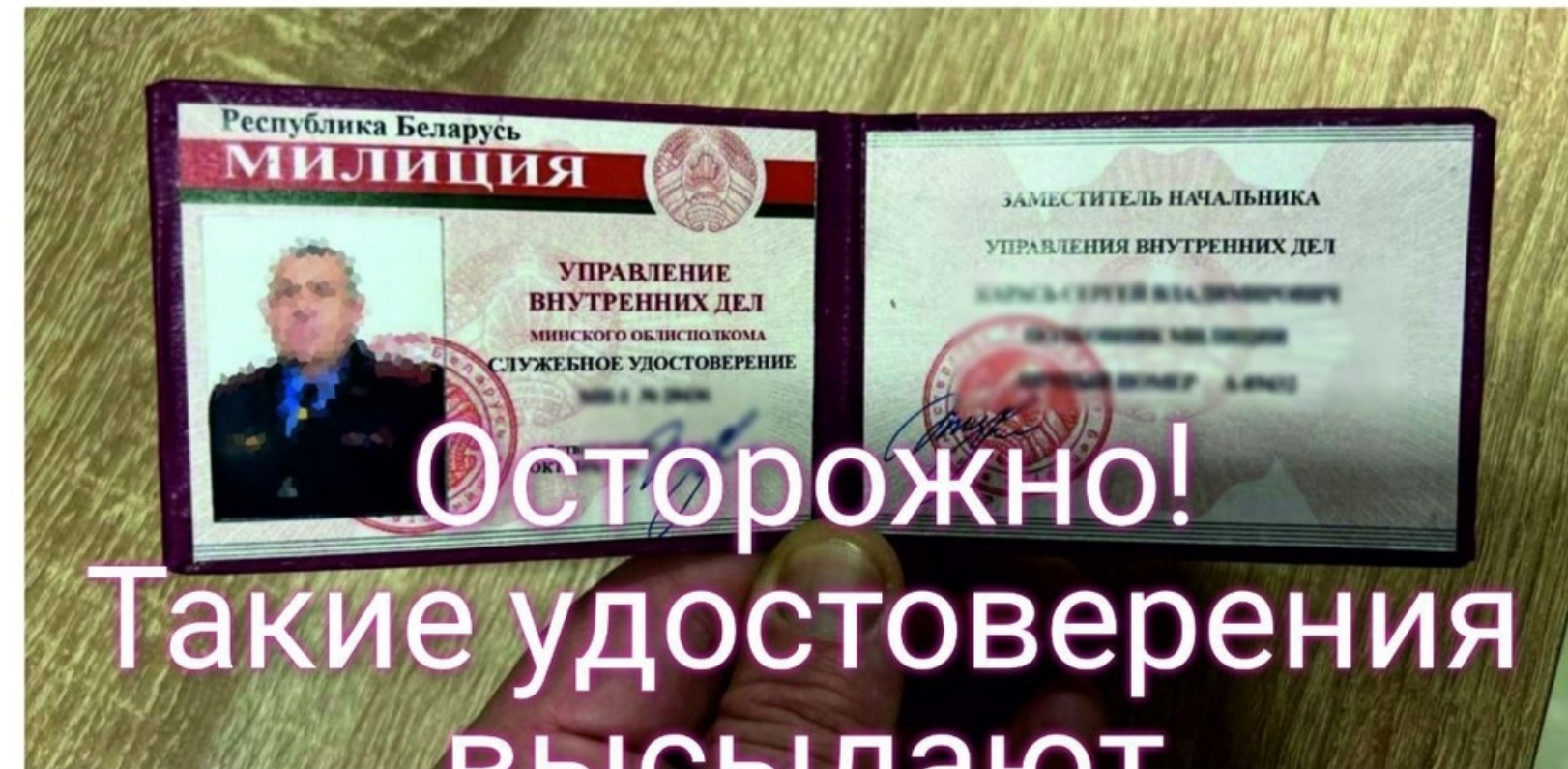
ВИШИНГ



Суть схемы

Мошенники используют психологические уловки, играют на чувствах, сначала угрожают или сообщают о проблеме, потом предлагают помощь в ее решении.

Потом убеждают установить программное обеспечение и передать код регистрации, или получить кредит и перевести деньги на “защищенный” счет.



Создают фейковый магазин или аккаунт на торговой площадке

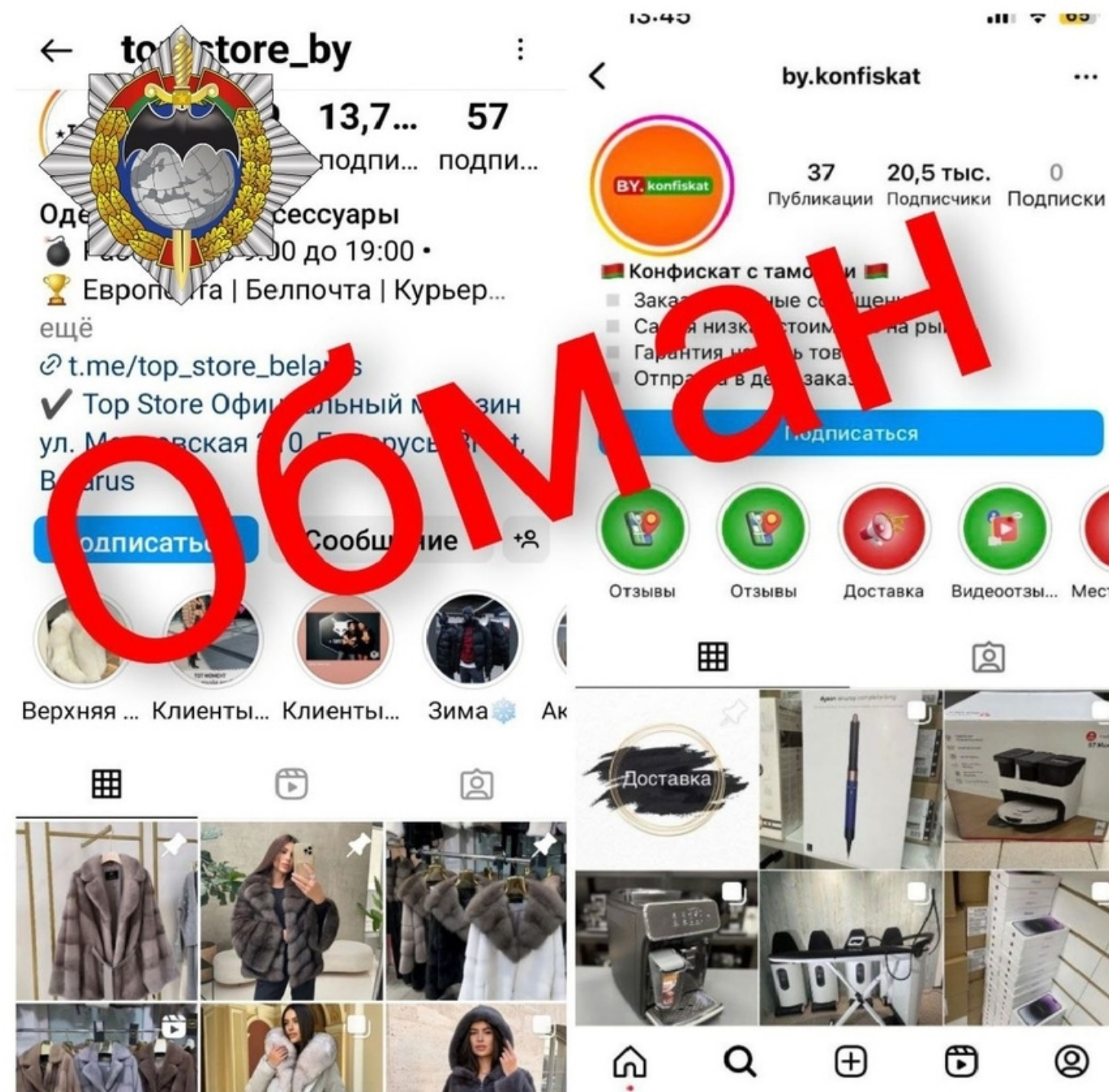
Суть схемы

Мошенники создают странички в соцсетях и на торговых площадках.

Размещают фото товара по заниженной стоимости.

И под различными предложениями убеждают перевести денежные средства.

Рекомендуется проверить существование магазина, **позвонив по белорусскому номеру.**



Создают фейковые сайты криптобирж или инвестиционных платформ.

Суть схемы

Мошенники создают сайты криптобирж или инвестиционных платформ.

Подыскивают заинтересованных в пассивном доходе людей, готовых вложить реальные деньги в фейковую биржу, якобы под «руководством куратора».

На деле оказывается, что заработок, видимый на экране, всего лишь нарисованный.

Легких денег НЕ БЫВАЕТ.

Реклама инвестиций работает по принципу финансовой пирамиды.

The screenshot shows a website designed to look like an official Gazprom investment platform. It features a dark blue header with the title 'Почему это выгодно для обычных граждан' (Why it is profitable for ordinary citizens) and a list of benefits: 'Значительная прибыль при минимальных рисках' (Significant profit at minimal risk), 'Один из самых доходных активов' (One of the most profitable assets), and 'Быстрый вывод средств на любую карту банка Беларуси' (Fast withdrawal of funds to any Belarusian bank card). To the right, a blue box asks 'Что нужно сделать, чтобы начать зарабатывать с Газпром Инвест уже сейчас?' (What do you need to do to start earning with Gazprom Invest now?) and lists steps: 'Зарегистрироваться на данном сайте в форме выше' (Register on this site in the form above), 'Дождаться звонка от консультанта компании Газпром Инвест и подтвердить регистрацию' (Wait for a call from a Gazprom Invest consultant and confirm registration), and 'Выбрать желаемую сумму на счет и уже через 30 дней получить первый доход' (Choose the desired sum on the account and receive the first income after 30 days). Below this, a photo of Alexey Miller is shown with his name and title: 'Алексей Миллер, председатель правления совета директоров ПАО «Газпром»' (Alexey Miller, Chairman of the Board of Directors of PJSC 'Gazprom'). The text continues: 'Мы приняли решение открыть доступ к торговле газом для граждан Беларуси, поскольку это будет выгодно и для Газпрома, так и для белоруссов.' (We have decided to open access to gas trading for Belarusian citizens, as it will be profitable for both Gazprom and Belarusians.) and 'Дело в том, что на данный момент российский газ становится самым востребованным на мировом рынке. Во всех странах мира стремительно растет спрос на его покупку. По этой причине мы решили увеличить объемы производства газа в 4 раза и привлечь людей со всей Беларуси в качестве инвесторов.' (The thing is, at the moment Russian gas is becoming the most demanded on the world market. In all countries, the demand for its purchase is growing rapidly. For this reason, we decided to increase gas production 4 times and attract people from all over Belarus as investors.) It also states: 'Поскольку цены на газ сейчас быстро меняются, все, кто участвуют в проектах Газпрома, получают в среднем по \$800-\$8,500 дохода ежемесячно.' (Since gas prices are changing rapidly now, everyone who participates in Gazprom projects receives an average income of \$800-\$8,500 per month.) A blue button at the bottom says 'Проконсультироваться' (Consult). A large, diagonal 'ФИШИНГ' (Phishing) watermark is overlaid across the entire image.

Создают фейковые сайты банковских организаций.

Суть схемы

Фишинг.

Способ, когда мошенники завладевают персональными данными и совершают хищение денежных средств.

Мошенник точно копирует настоящий и создает фишинговый сайт.

Интернет-адреса белорусских организаций должны быть расположены в национальном сегменте Интернета – доменной зоне «BY».

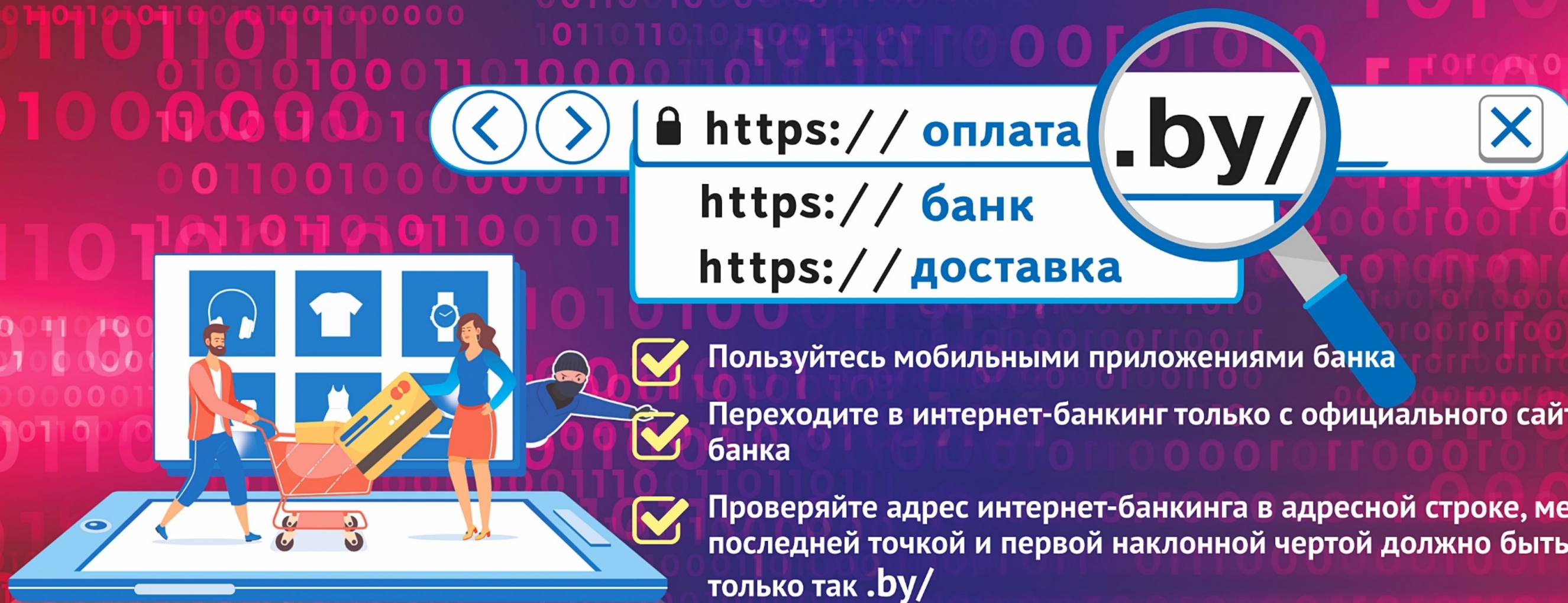
Всегда проверяйте адрес страницы, где вводите личные данные.

The screenshot shows a phishing website designed to look like the official site of 'Белагропромбанк' (Belarusian Agricultural Bank). The browser's address bar shows the URL 'agrobels-refferal.su', which is circled in red. A red arrow points from the browser's address bar to the URL. The website features a header with the bank's logo and name. Below the header, there is a large orange banner with the text 'Получите 100 BYN!' (Get 100 BYN!) and a registration form with fields for 'Номер телефона:' (Phone number) and 'Идентификационный номер:' (Identification number). Below the form is a button labeled 'ЗАРЕГИСТРИРОВАТЬСЯ' (REGISTER). At the bottom, there are three promotional banners: 'Кредит ОНЛАЙН ЛЕГКИЕ ПОКУПКИ' (Credit ONLINE EASY PURCHASES), 'КРЕДИТ НА РАЗ' (CREDIT ON THE SPOT), and 'вклад ПЛЮС К СТАБИЛЬНОСТИ' (deposit PLUS TO STABILITY). A small text block at the bottom of the page contains a disclaimer: 'Внимание! В случае возникновения проблем с отображением отдельных страниц системы «Интернет-банкинг» рекомендуем произвести в используемом браузере удаление временных файлов Интернета (кэш), файлов (cookie). Для браузеров Internet Explorer, Mozilla Firefox, Opera, Google Chrome нажмите Ctrl+Shift+Del, выберите в экранной форме соответствующие отметки и нажмите удалить. Информировать, что ранее максимальная длина пароля составляла 10 символов, более длинные пароли обрезаются. В настоящий момент длина пароля увеличена до 20 символов. Если Вы использовали ранее длинный пароль, а сейчас не можете войти в систему - попробуйте вводить первые 10 символов своего пароля.'

Внимательно проверяйте адрес страницы, где вводите личные данные!

Это поддельная страница!

ПОЛЬЗУЙСЯ БЕЗОПАСНО



УПРАВЛЕНИЕ
ПО ПРОТИВОДЕЙСТВИЮ
КИБЕРПРЕСТУПНОСТИ
УВД ВИТЕБСКОГО
ОБЛИСПОЛКОМА

- ✓ Пользуйтесь мобильными приложениями банка
- ✓ Переходите в интернет-банкинг только с официального сайта банка
- ✓ Проверяйте адрес интернет-банкинга в адресной строке, между последней точкой и первой наклонной чертой должно быть только так .by/
- ✓ Активируйте на карте, используемой для онлайн-платежей, услугу 3-D Secure (подтверждение платежей SMS-кодом)
- ✓ Не переходите в интернет-банкинг по ссылкам в поисковых системах
- ✓ Не используйте SMS-коды от банка и код с обратной стороны карты для получения денежных средств
- ✓ Не переходите по ссылкам из сообщений для доступа к интернет-банкингу и иным сервисам или услугам

Информационная безопасность



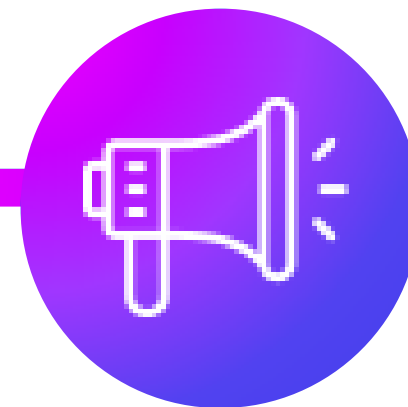
Сложные пароли

К разным сервисам разные пароли
Состав пароля
Менеджер паролей
Облачные пароли к сервисам



Коды и ключи

Коды в совокупности с другими данными предоставляют доступ к сервисам и, в некоторых случаях, дают возможность оформить кредит.



Денежные переводы

Фейковые магазины предлагают перевести предоплату за товар на счет или БПК.
Мошенники под различными предложениями “вытягивают” из жертв деньги.



Личные данные

Распространение личных данных способствует совершению преступлений. Мошенники используют нейросети и создают дипфейки (голосовые или видеоизображения).

Киберпреступность несовершеннолетних



4'

по ст. 340 УК (Заведомо ложное сообщение об опасности), 14, 14, 15 лет, все учащиеся витебских школ.

Вплоть до 7 лет лишения свободы.

*12 летний – не достиг возраста привлечения.

1

по ст. 209 УК (Мошенничество), 17 лет, учащийся колледжа.

Вплоть до 10 лет лишения свободы.

6

по ст. 222 УК (Незаконный оборот средств платежа).

Вплоть до 10 лет лишения свободы.

2

по ст. 212 УК (Хищение имущества путем модификации компьютерной информации), учащиеся средней школы области.

Вплоть до 12 лет лишения свободы.



Управление по противодействию
киберпреступности
криминальной милиции
УВД Витебского облисполкома



Telegram-канал
“Цифровая грамотность”
@cifgram

МОШЕННИКИ МОГУТ ПРЕДСТАВИТЬСЯ

- работники банка-сотрудники
- представители органов
- родственники, попавшие в беду
- продавец или покупатель

НЕ ВОСПРИНИМАЙТЕ НИКАКИХ ДЕЙСТВИЙ ПО ПРОСЬБЕ ТРЕТЬИХ ЛИЦ!

- ✓ НЕ ПЕРЕДАВАЙТЕ ДАННЫЕ КАРТЫ И КОДЫ ИЗ SMS-СООБЩЕНИЙ ОТ БАНКА, ПОЛУЧЕН ИЛИ ПОЛУЧИТЕ В СЕРВИСАХ
- ✓ НЕ УСТАНАВЛИВАЙТЕ ПРОГРАММЫ ПО ПРОСЬБЕ ТРЕТЬИХ ЛИЦ ИЛИ СООБЩАЙТЕ КОДЫ РЕГИСТРАЦИИ
- ✓ НЕ ОФОРМЛЯЙТЕ КРЕДИТЫ ПО ПРОСЬБЕ ТРЕТЬИХ ЛИЦ
- ✓ НЕ ПЕРЕВОДИТЕ ДЕНЕГ НА «ЗАКРЫТЫЙ СЧЕТ»
- ✓ НЕ ПЕРЕДАВАЙТЕ ДЕНЕГ ДЛЯ ПОДСУДЕННЫХ, ЧЕРЕЗ ЭТО НЕКОМУ!

ПОЛЬЗУЙСЯ БЕЗОПАСНО

«банк».by

- ✓ Пользуйтесь официальным приложением банка
- ✓ Переходите в интернет-банк только с официального сайта банка
- ✓ Проверьте адрес интернет-банка и в адресной строке, между последней точкой и первой буквой четкой должна быть точка «.by»!
- ✓ Авторизуйтесь на сайте, используя для входа логин, пароль и 3-D Secure подтверждение кодом SMS кода
- ✓ Не переходите в интернет-банк по ссылке в электронных письмах
- ✓ Не используйте SMS коды от банка и код с одноразовым старшим картой для получения денежных средств
- ✓ Не переходите по ссылке из сообщения для доступа к интернет-банку и не используйте эти услуги

БЫТЬ ХАКЕРОМ -

НЕ РАЗВЛЕЧЕНИЕ,
А ПРЕСТУПЛЕНИЕ

УГОЛОВНАЯ ОТВЕТСТВЕННОСТЬ ЗА КИБЕРПРЕСТУПЛЕНИЯ НАСТУПАЕТ:

- статья 210 УК: Иллюзии, иллюзии! Пусть кодифицирует компьютерный информации, не выводит вплоть до лишения свободы на срок до 12 лет
- статья 340 УК: Заведомо ложные сообщения об опасности, не выводит вплоть до лишения свободы на срок до 7 лет
- статья 332 УК: Незаконный доступ к компьютерной информации, не выводит вплоть до лишения свободы на срок до 10 лет
- статья 349 УК: Незаконный доступ к компьютерной информации, не выводит вплоть до лишения свободы на срок до 7 лет

ВНИМАНИЕ! ЗАЩИТИТЕ СЕБЯ ОТ КИБЕРМОШЕННИЧЕСТВА!

МОШЕННИК МОЖЕТ ПРЕДСТАВИТЬСЯ:	НАЗВАТЬ ПРИЧИНУ ЗВОНКА:
сотрудники банка	если кредит-кредит
сотрудники правоохранительных органов	по поводу счета
родственники или друзья из чрезвычайной ситуации	обнаружены мошеннические операции
	подтверждение информации
	доверенности на операции на счету

МОШЕННИК МОЖЕТ ПОПРОСИТЬ:

- карты, коды, SMS-коды, данные в транзитном или на обратном пути, код на SMS-сообщениях
- коды, в том числе интернет-банк и переводы на номера телефонов
- коды, или подтвердить, чтобы не было проблем
- коды, разработанные мошенниками
- коды, разработанные мошенниками
- информацию кредит в банке
- перевести деньги на специальный счет

НЕ СООБЩАЙТЕ ДАННЫЕ КАРТЫ И КОДЫ ИЗ SMS
НЕ УСТАНАВЛИВАЙТЕ ПРОГРАММЫ ПО ПРОСЬБЕ ТРЕТЬИХ ЛИЦ
НЕ ОФОРМЛЯЙТЕ КРЕДИТЫ
НЕ ПЕРЕВОДИТЕ ДЕНЕГ НА «ЗАКРЫТЫЙ СЧЕТ»
Большая информация на сайте цифровой грамотности и Telegram-канал

КИБЕР-ВИКТОРИНА!

ПРОЙДИ ТЕСТ

ПОДПИШИСЬ НА КАНАЛ

ОСТОРОЖНО! МОШЕННИКИ!

ПО ПРОСЬБЕ НЕЗНАКОМЫХ ЛИЦ:

- ✓ НЕ сообщайте данные карты и коды из SMS-сообщений от банка, логины и пароли доступа к сервисам
- ✓ НЕ устанавливайте программы, не передавайте коды регистрации
- ✓ НЕ оформляйте кредиты
- ✓ НЕ переводите деньги на «закрытый счет»

ЕСЛИ ВЫ ПОЛУЧАЕТЕ ЗВОНОК ИЗ «БАНКА», ЗАВЕРШАЙТЕ РАЗГОВОР И ПОДВЕДИТЕ В БАНК
Установите в телефоне защиту от мошенников

БУДЬТЕ ВДИТЕЛЬНЫ!
НЕ СТАНЬТЕ ЖЕРТВОЙ ОБМАНА!