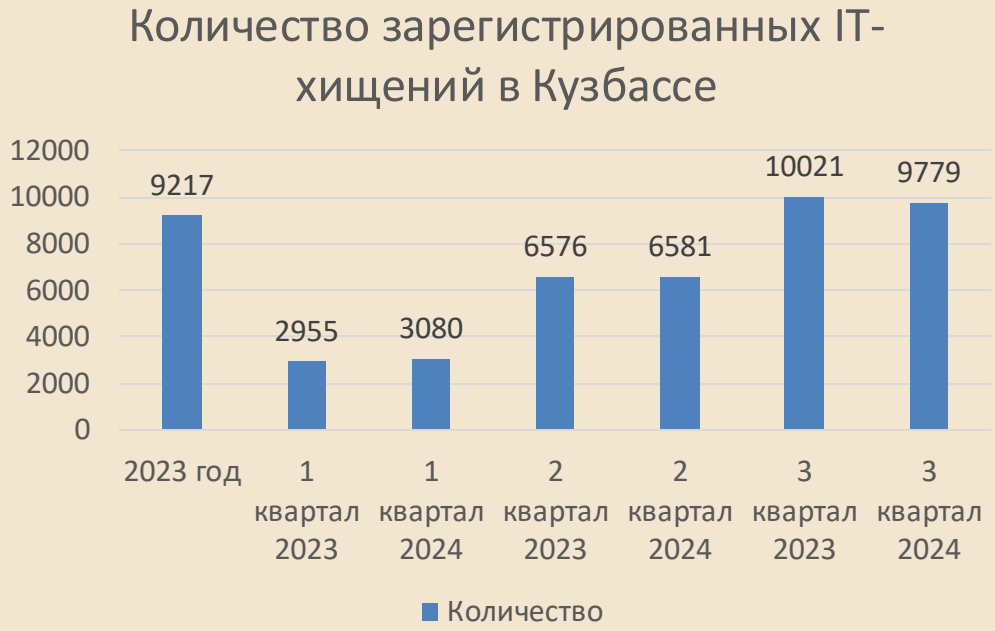
«Современные способы кибермошенничеств и методы противодействия»

Заместитель начальника отдела Управления уголовного розыска ГУ МВД России по Кемеровской области – Кузбассу
подполковник полиции
Бутенко Максим Александрович

IT-хищения


Количество зарегистрированных IT-хищений в Кузбассе
12000
10000
8000
6000
4000
2000
0
9217
2955
3080
6576
6581
10021
9779
2023 год
1 квартал 2023
1 квартал 2024
2 квартал 2023
2 квартал 2024
3 квартал 2023
3 квартал 2024
Количество


Причиненный ущерб от IT-хищений в Кузбассе
3.0
2.5
2.0
1.5
1.0
0.5
0.0
2.6
0.473
0.512
1.07
1.29
1.56
1.85
2023 год
1 квартал 2023
1 квартал 2024
2 квартал 2023
2 квартал 2024
3 квртал 2023
3 квартал 2024
Сумма, млрд Р.

Основные способы кибермошенничеств:

- Звонок лжесотрудника банка, правоохранительных органов, представителя операторов сотовой связи, сервиса «Госуслуги Энергосбыта, Пенсионного фонда и др.»;
- Звонок, сообщение псевдоруководителя;
- Покупка/продажа товаров/услуг в сети Интернет;
- Вложения в инвестиционные проекты, биржи, тотализаторы;
- Хищение с утраченной (похищенной) банковской карты (счета);
- Взлом учетной записи, аккаунта, личного кабинета;
- Родственник попал в ДТП.

ЭМОЦИИ, КОТОРЫЕ ВЫЗЫВАЕТ ИНФОРМАЦИЯ ОТ ТЕЛЕФОННЫХ МОШЕННИКОВ

ПОЛОЖИТЕЛЬНЫЕ

- **РАДОСТЬ НАДЕЖДА**
- **ЖЕЛАНИЕ ПОЛУЧИТЬ ДЕНЬГИ**

ОТРИЦАТЕЛЬНЫЕ

- **СТРАХ ПАНИКА**
- **ЧУВСТВО СТЫДА**

«Вы выиграли крупную сумму денег»

«Вам положены социальные выплаты»

«Пенсионный фонд рад сообщить вам о перерасчете вашей пенсии, вам положена выплата в размере…»

«С вашего счета списали все деньги»

«Ваш родственник попал в аварию и сбил человека»

«Вас беспокоит следователь Следственного комитета, вы участник уголовного дела о… коррупции или…»

ТЕЛЕФОННЫЕ МОШЕННИКИ: РАСПРОСТРАНЕННЫЕ СХЕМЫ

«ЛЖЕСОТРУДНИК ЦЕНТРОБАНКА (БАНКА РОССИИ)»

«По вашей карте зафиксирована сомнительная операция. Для сохранности денег вам нужно перевести их на «безопасный» («специальный») счет в Центробанке»

«ПРЕДСТАВИТЕЛЬ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ (МВД, ФСБ, СК РФ)»

«Следователь Следственного комитета.
Вы являетесь свидетелем по уголовному делу»

«Иванов В.В., капитан полиции. По вашему паспорту оформлен кредит и указана ваша карта. Нам необходимо уточнить ее реквизиты»

ПОД ВИДОМ ПРЕДСТАВИТЕЛЕЙ СОТОВЫХ ОПЕРАТОРОВ

«ПРЕДСТАВИТЕЛЬ СОТОВОГО ОПЕРАТОРА»

«На Ваш телефонный номер была подана заявка на смену оператора»
«Для обеспечения безопасности необходимо сменить пароль в личном кабинете»

Злоумышленник получает SMS-код, после чего получает доступ к номеру жертвы, а, следовательно, возможность в личные кабинеты банков, портала госуслуг и других сервисов.

ПОД ВИДОМ СОТРУДНИКА СОЦИАЛЬНОГО ФОНДА

«СОТРУДНИК СОЦИАЛЬНОГО ФОНДА»

«В ходе проверки зафиксирован неучтенный стаж, предлагаем оформить официальное заявление на перерасчет пенсии в сторону ее увеличения»

Злоумышленник получает SMS-код, после чего получает доступ к порталу «Госуслуги», а также к мобильному банку.

ПОД ВИДОМ СОТРУДНИКА ЭНЕРГОСБЫТ

«СОТРУДНИК ЭНЕРГОСБЫТ»

«Необходимо заменить электросчетчик»
«Необходимо проверить электросчетчик»
«Необходимо провести перерасчет платежей»
«необходимо изменить номер счета для оплаты электроэнергии»

Злоумышленник убеждает установить приложение «Энергосбыт» в результате чего получает доступ в личный кабинет банка и Госуслуг, тем самым похищая денежные средства

Варианты использования фейковой учётной записи Telegram

«Злоумышленник

под видом другой учётной записи»

Иван Сергеевич, здравствуйте. Как ваше здоровье? Как работа? Я пишу вам по делу. Хочу вас предупредить, что сегодня Вам будет звонить Нестеров Алексей Александрович, который курирует наше учреждение.
У него есть к вам несколько вопросов. Звонок очень важный, обязательно пообщайтесь!

Создание фейковой учётной записи, не имеющей отношение к пользователю. Ведение переписки от имени другого лица.

Варианты использования захваченной учётной записи мессенджера

«Злоумышленник

под видом НО организации»

Добрый день. Это Станислав Викторович начальник вашего отдела.
С вами не может связаться наш генеральный директор Андрей Валерьевич
и просит ему перезвонить. (сообщает номер)

Злоумышленник используя чужую учетную запись указывает в ней анкетные данные действующего руководителя организации и от его имени связывается с сотрудниками данной организации и злоупотребляя их доверием переводит на диалог с подельниками.

«Злоумышленник

под видом ГД организации»

Добрый день! Это Андрей Валерьевич! Наш разговор носит строго конфиденциальный характер, разглашение сведений несет за собой уголовную ответственность и будет расценено как содействие СБУ. В руки СБУ попали личные данные более 2500 сотрудников нашей организации, в том числе доступы к банковским счетам, и ваша кандидатура избрана для оказания содействия в их поиске. В настоящий момент злоумышленники оформляют кредиты на сотрудников нашей организации и все имеющиеся средства выводят предположительно в поддержку ВСУ. Для начала, чтобы пресечь попытку списания ваших денежных средств, вам необходимо исчерпать свой кредитный лимит и все имеющиеся на расчетных счетах денежные средства перевести на резервный счет, который я вам сообщу.

Как только жертва связывается с подставным генеральным директором, злоумышленник всеми возможными способами пытается завладеть денежными средствами жертвы.

Банк России

МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ

НЕ ОТДАВАЙТЕ КАРТУ В ПЛОХИЕ РУКИ!

КТО ТАКИЕ ДРОППЕРЫ

Это сообщники злоумышленников, которые выводят и обналичивают похищенные у граждан деньги.

ЧЕМ ЗАНИМАЮТСЯ ДРОППЕРЫ

- Получают на свои карты деньги от незнакомцев и передают их другим лицам – наличными или переводом
- Предоставляют злоумышленникам банковские карты или доступ к онлайн-банку
- Принимают наличные деньги от неизвестных людей, вносят их на свои счета для последующего перевода

ГДЕ И КАК ИЩУТ ДРОППЕРОВ

Основной канал – интернет (социальные сети, мессенджеры, электронная почта).

Злоумышленники обещают гарантированный доход без официального трудоустройства и удаленный режим работы. Опыт работы и специальные навыки их не интересуют.

Единственное требование к дропперу – наличие банковских карт.

ЧТО ГРОЗИТ ДРОППЕРАМ

- Дропперы попадают в базу данных Банка России
- Банки ограничивают им доступ к онлайн-банку и картам
- Для многих граждан такая «работа» заканчивается уголовным наказанием

Как не попасться на уловки мошенников

Чтобы обезопасить свои деньги от злоумышленников, придерживайтесь главных принципов кибербезопасности:

1 Держите в секрете конфиденциальные данные

Никому не сообщайте полные реквизиты карты, включая срок ее действия и три цифры с оборота, а также пароли и коды из банковских уведомлений. Ими интересуются только мошенники.

2 Не спешите выполнять инструкции незнакомцев

Не переходите по ссылкам неизвестных отправителей, не переводите деньги по первому требованию (даже если вас об этом просит друг или родственник – возможно, это мошенники, взломавшие их аккаунты). Не перезванивайте на неизвестные номера и не вводите данные карты на подозрительных сайтах.

3 Перепроверяйте информацию

Получили внезапный тревожный звонок «из банка»? Не верьте собеседнику на слово. Чтобы прояснить ситуацию, положите трубку и вручную наберите номер банка, указанный на вашей карте или на его официальном сайте.

4 Защищайте данные на своих устройствах

Установите антивирус на все гаджеты, которыми пользуетесь, и не забывайте его обновлять. Ставьте надежные пароли на вход в аккаунты, к которым привязана ваша банковская карта. Используйте биометрическую разблокировку для телефона – мошенники не смогут ее подделать, если вы потеряете устройство.

Банк России

Финансовая культура

Узнай больше на fincult.info

ПОМНИ!
Перевел деньги мошенникам – помог врагу!