УПРАВЛЕНИЕ ВНУТРЕННИХ ДЕЛ
ГОМЕЛЬСКОГО ОБЛИСПОЛКОМА
КРИМИНАЛЬНАЯ МИЛИЦИЯ
УПРАВЛЕНИЕ ПО ПРОТИВОДЕЙСТВИЮ
КИБЕРПРЕСТУПНОСТИ

ПЛАН-КОНСПЕКТ

Тема:

«*Как уберечь пожилых граждан от мошенников в сети Интернет!*»

Гомель, 2023 год

Как уберечь пожилых граждан от мошенников в сети Интернет!

Стать жертвой мошенников может любой человек, но чаще всего на удочку попадаются пенсионеры. Злоумышленники умело заговаривают пожилых людей, убеждают в своей правоте, и те отдают им свои сбережения. Развод на деньги в интернете – один из излюбленных злоумышленниками методов обмана стариков.

В Гомельской области в 2022 году потерпевшими от хищений имущества путем модификации компьютерной информации (ст. 212 УК Республики Беларусь) стали 174 пенсионера (12,7% об общего количества потерпевших по данным преступлениям). Мошенники заполучили денежные средства пенсионеров, используя метод «вишинг» (когда звонят сотрудники якобы банка или милиции) – 56,3%, после перехода пожилыми гражданами по фишинговым ссылкам в сети Интернет и ввода своих реквизитов банковских карт либо паспортов – 20,1%, после хищения либо утери банковских карты пожилым гражданином – 23,6%.

Почему пенсионеры — самая уязвимая категория?

- Людьми преклонного возраста легко манипулировать. Они наивны и доверчивы, их проще ввести в заблуждение, запугать.
- Пенсионеры плохо разбираются в новых технологиях, не могут проверить информацию в интернете.
- Людям преклонного возраста, не привыкшим пользоваться банкоматами и картами, ничего не стоит выдать секретные данные для доступа к счёту.
- Пожилые люди привыкли безоговорочно доверять каждому, кто произнесёт «соцслужба», «милиция», «собес» или волшебное слово «бесплатно».
- У пенсионеров, особенно одиноких, ввиду изолированного образа жизни обострена потребность в общении, они охотно идут на контакт.

Мошенники всегда убедительны и могут ввести в заблуждение даже самого подозрительного пенсионера. Уважительно разговаривают, доходчиво объясняют, покоряют желанием помочь. При таком отношении сложно не довериться.

УПК КМ УВД Гомельского облисполкома

Какие сценарии наиболее популярны и как от них уберечь бабушек и дедушек.

Звонок от сотрудника банка (собственной безопасности банка).

Аферист звонит по телефону и представляется сотрудником безопасности банка. Сообщает, что с карты клиента был совершён платёж, который вызвал подозрения. Уточняет, делал ли человек такую операцию (естественно, нет). Предлагает вернуть деньги, для чего просит сообщить номер карты, срок действия и код безопасности — то есть то, что сообщать нельзя. Нередко мошенники отправляют SMS с текстом: «Ваша карта заблокирована, отправьте код для разблокировки», «Вам положена компенсация, для получения пришлите код». Также под надуманным предлогам убеждают установить программу «ANY DESK», говоря, что она нужна для отмены незаконного платежа, а потом с помощью данной программы осуществляют переводы денежных средств с банковских карт потерпевших.

Также звонивший может представится сотрудником милиции или следственного комитета, и предложить поучаствовать в «СПЕЦОПЕРАЦИИ» по поимке преступников из банка. В такой ситуации необходимо ПОЛОЖИТЬ ТРУБКУ ТЕЛЕФОНА и самому перезвонить в милицию. Сотрудники правоохранительных органов никогда не предлагают гражданам участвовать в каких-либо операциях. Вы разговаривали с мошенниками!

Кроме этого, мошенники могут предлагать выгодный вклад или перевод сбережений на него, либо пугают блокировкой счёта и риском потерять накопленное. В надежде получить выплату или защитить свои деньги пенсионер раскрывает секретную информацию. Мошенник опустошает карту. Только потом человек понимает, что его обманули.

Как избежать афер с лжебанкирами:

- Не вступайте в переговоры с незнакомцем. Положите трубку и самостоятельно обратитесь в банк по номерам, указанным на официальном сайте.
- Не паникуйте, если вам сообщают о блокировке счета. Позвоните в банк по номеру, указанному на сайте или на карте.
- Не обращайте внимание на обещания лёгких денег или выгоды без усилий.
- Ни под каким предлогом, **ОСОБЕННО ПО ТЕЛЕФОНУ**, не передавайте и не сообщайте платежные реквизиты, полный номер карточки и срок ее действия, логин и пароль к интернет-банку, иную персональную информацию.
- Если собеседник торопит вас или спрашивает смс-код, то вы говорите с мошенником.
- Не переходите по неизвестным ссылкам, которые Вам предоставил неизвестный, и не посещайте интернет-ресурсы сомнительного содержания.
- Внимательно читайте сообщения из банка. Мошенники используют имена отправителей, похожие на названия банков, и допускают ошибки в тексте.
- В случае утери или кражи карты необходимо незамедлительно заблокировать ее по телефону, или обратиться в банк.
- Ни под каким предлогом не отправляйте реквизиты карты фотоизображения по сети Интернет.
- Не сообщайте данные, полученные в виде SMS-сообщений: сеансовые пароли, код авторизации, пароль «3-D Secure» и т.д..
- Применяйте все доступные способы защиты, предлагаемые банками (двухфакторная авторизация, смс-оповещение о расходных операциях, лимит снятия денежных средств и др.).

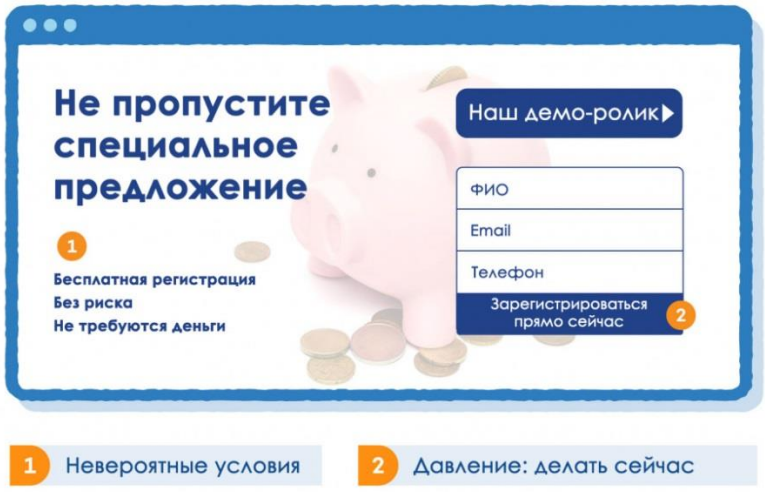
Звонки из милиции, следственного комитета, прокуратуры и т.п.

УПК КМ УВД Гомельского облисполкома

Простая схема манипулирования людьми: сотрудник милиции сообщает по телефону, что родственник пенсионера попал в ДТП или совершил преступление. Чтобы избежать уголовной ответственности, нужна взятка. Требуется перевод денег или их передача курьеру. **Важно помнить и предупредить близких: если поступает подобный звонок, в первую очередь нужно лично позвонить «пострадавшему» и убедиться, что у него всё хорошо. Обратитесь в милицию, чтобы пресечь противоправную деятельность мошенников.**

Онлайн-инвестиции

Многим пожилым людям при выходе на пенсию требуются дополнительные доходы или им необходима помощь в управлении своими сбережениями. Аферы с онлайн-инвестициями как раз нацелены на этих людей, обещая хорошую отдачу от их инвестиций. Стоит ли говорить, что как только пожилые люди переводят свои средства мошенникам, то они их больше никогда не увидят снова.



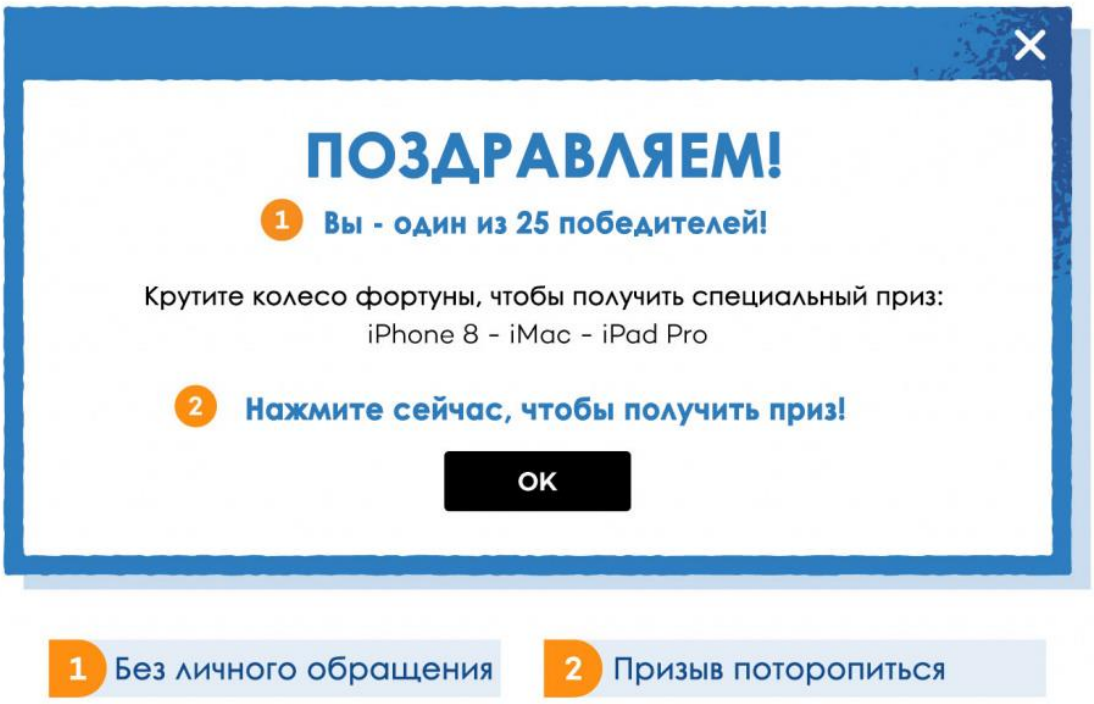
УПК КМ УВД Гомельского облисполкома

Как избежать афер с онлайн-инвестициями:

- Остерегайтесь обещаний получить огромную прибыль без риска.
- Избегайте предложений, которые заставляют вас принимать быстрые действия.
- Проконсультируйтесь по поводу инвестиций в своем банке или у доверенного финансового советника.
- Убедитесь, что рекламируемый инвестиционный фонд имеет все необходимые лицензии и регистрации.

Ложные выигрыши

Приходит SMS с информацией о выигрыше денег, машины, ценного приза. Для получения «выигрыша» аферисты просят перевести сумму в счёт уплаты налогов или пошлин. И как только получают деньги, исчезают.

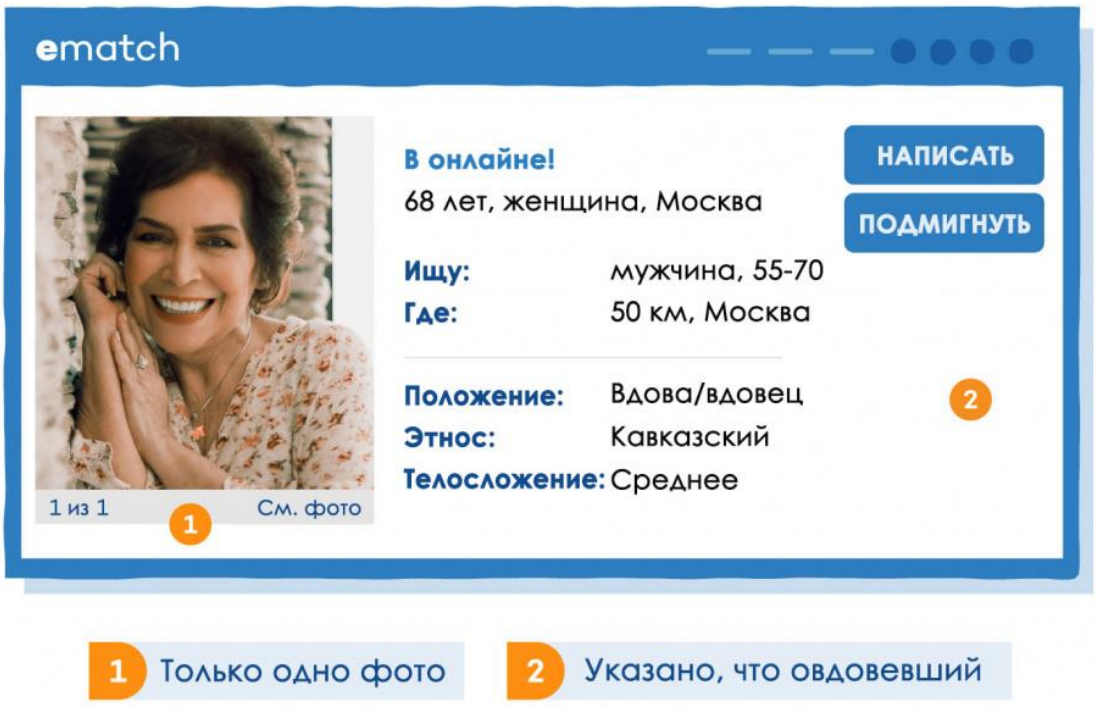


Как избежать афер с лотереями:

- Помните, что вы не можете выиграть в лотерею, если вы в ней никогда не участвовали.
- Имейте в виду, что никто не раздает деньги просто так.
- Никогда не передавайте данные доступа к вашему банковскому счету через Интернет.

Онлайн-знакомства.

Интернет может быть отличным местом для пожилых людей, желающих найти новые знакомства или даже любовь. Круг знакомств в Интернете огромный, но, к сожалению, в нем водится очень много мошенников. Кэтфишинг (catfishing) – это когда кто-то создает в Интернете несуществующего человека (поддельный профиль) и заводит знакомства с доверчивыми людьми с той целью, чтобы обманом выманить у них деньги. Они придумывают целый сценарий, в котором им нужно будет занять деньги (например, для члена семьи, который заболел, или для полета на самолете, чтобы встретиться с вами и познакомиться лично). Многие пожилые люди становятся жертвами этой аферы, потому что они ищут общения и могут быть слишком доверчивыми.



Как избежать афер с онлайн-знакомствами:

- Ищите несоответствия в профиле нового знакомого.
- Будьте осторожны с теми людьми, кто пытается установить с вами взаимоотношения.
- Расскажите своей семье или друзьям о новом знакомстве, чтобы они могли проверить профиль этого человека.
- Никогда не перечисляйте деньги кому-либо, с кем вы познакомились в Интернете.

Медицинский обман

В период продолжающейся пандемии этот вид манипуляции людьми стал весьма действенным. Аферист звонит по телефону, представляется сотрудником поликлиники и говорит, что государство обязало пенсионеров пройти обследование на COVID-19, настаивает на покупке лекарства для профилактики.

«Сотрудник» убедителен, чётко отвечает на вопросы, использует медицинскую терминологию. Человек верит, переводит деньги и ждёт медработника, который привезёт лекарство и проведёт обследование на дому. Естественно, никто не приезжает, после звонка в поликлинику факт обмана подтверждается.

Ещё вариант: звонок из «поликлиники», пугают — у вас обнаружено серьёзное заболевание, нужны лекарства и медицинские приборы. Мы доставим.

Как избежать афер с лекарствами:

- Не верьте рекламе, которая обещает Вас вылечить от всех болезней, не верьте в чудо-средство, чудо-лекарство, чудо-продукт, чудо-БАД от всех болезней.
- Если Вы сомневаетесь в предложении и в целесообразности покупки, проконсультируйтесь с Вашим лечащим врачом, у которого Вы наблюдаетесь.
- Проверьте, не продается ли БАД, который Вам рекламировали и предлагали, в аптеке дешевле в 10-20 раз (гораздо дешевле).

УПК КМ УВД Гомельского облисполкома

- Никогда не принимайте консультации и рекомендации по лечению по телефону от «академиков», «профессоров», «врачей» клиник, институтов, больниц, в которых Вы не наблюдаетесь и которых не знаете лично.
- Никогда не переводите деньги людям, которых Вы не знаете лично и в которых не уверены.

Социальная помощь

Позвонив по телефону и представившись сотрудником соцзащиты или подобной организации, аферист сообщает пенсионеру, что ему положена какая-то доплата или надбавка. Очень часто могут ссылать на постановления президента или мэра города, добавляя «ну, вы же видели по телевизору». В общем, деньги ждут перевода, и нужно оплатить небольшую комиссию за него.

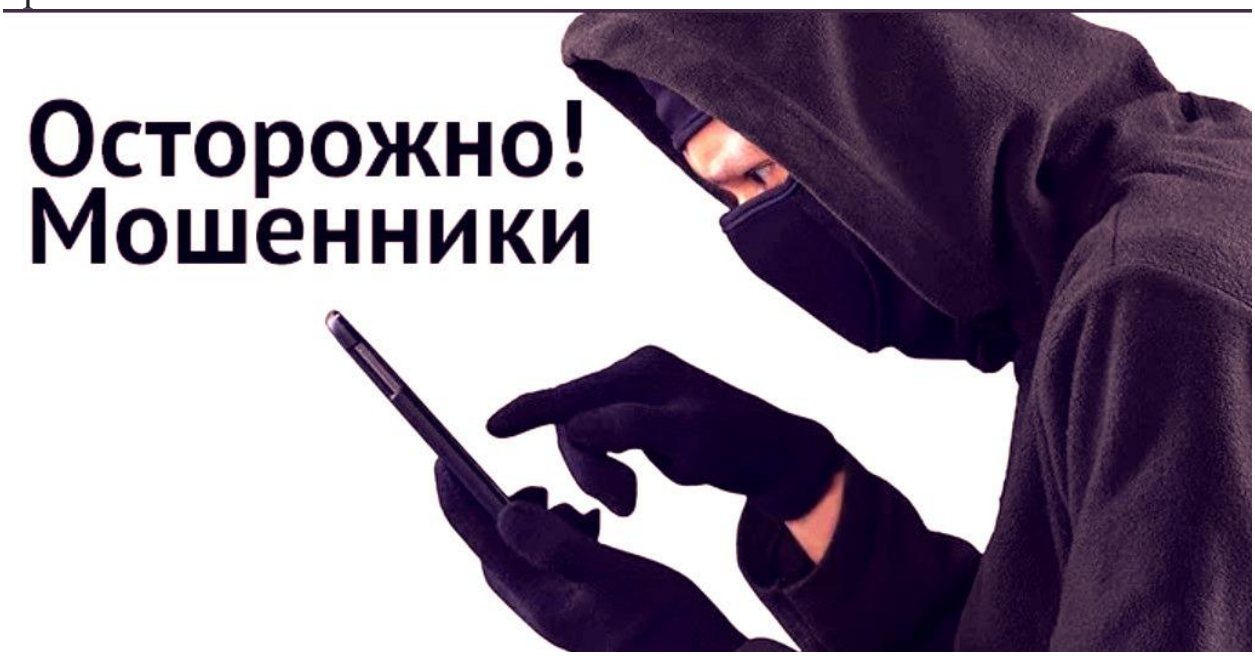
Как избежать афер с лжесоцслужбами:

- Критично отнеситесь к информации о предоставлении льгот и доплат.
- Перезвоните сами сотруднику, а лучше обратитесь лично в соцзащиту, и уточните о льготах, которые Вам положены.
- Никогда не перечисляйте деньги (комиссионный сбор) кому-либо, за обещание предоставить Вам денежные средства. Предоставляя доплаты, соцзащита не взымает никакую комиссию.
- Расскажите своей семье или друзьям о положенных льготах, чтобы они могли уточнить информацию у надежных источников.

УПК КМ УВД Гомельского облисполкома

Техническая поддержка.

Техническая поддержка мошенников начинается со всплывающего предупреждения о проблеме с компьютером. Всплывающее окно содержит номер телефона, куда можно позвонить. Поддельные сотрудники Microsoft или Apple отвечают на телефонные звонки и убеждают вас предоставить им доступ к вашему компьютеру, чтобы они могли решить проблему. Затем они либо получают доступ к вашему банку через ваш компьютер, либо запрашивают оплату за указанный «ремонт».



Как избежать афер с технической поддержкой:

- Не становитесь жертвой тех обращений к вам, когда вам говорят о том, что нужно срочно предпринять какие-то меры.
- Проверьте в поисковых системах номер телефона, чтобы убедиться в том, что он действительно принадлежит названной компании.
- Для устранения каких-либо поломок компьютера или установки обновлений (антивирусов и т.д.) обратитесь к специалистам самостоятельно, не пользуйтесь навязанными Вам телефонами.

Просьба денег от друга в социальных сетях.

Общаясь в социальных сетях с друзьями, мы иногда получаем сообщения от них тревожного характера (помоги на операцию, одолжи денег и т.д.). Помните, что это сообщение может быть написано мошенником со взломанной страницы Вашего знакомого.

Как избежать афер с поддельными друзьями:

- Свяжитесь по телефону с другом и убедитесь, он ли направлял Вам это сообщение.
- Если Вы не можете позвонить по телефону другу, ни в коем случае не переводите деньги на предоставленные Вам банковские карты или телефонные номера.

Руководствуясь данными правилами, Ваши деньги останутся при Вас! Берегите себя и своих близких!