«Кибербезопасность и профилактика
киберпреступности в Минской области»
(слайд №1).

Стремительное развитие цифровых технологий, переход к безналичным расчетам за приобретение товаров и услуг, размещение в сети Интернет персональных данных пользователей, стали следствием ежегодного увеличения количества регистрируемых киберпреступлений в 2 – 2.5 раза. Преступные группы активно используют в своей деятельности новейшие достижения науки и техники, применяют всевозможные компьютерные устройства и новые информационные технологии для совершения и сокрытия преступлений **(слайд №2)**.

Однако в 2021 году сложилась устойчивая тенденция снижении количества регистрируемых киберпреступлений. Так в январе-феврале 2022 года на территории Минской области зарегистрировано 320 киберпреступлений. В аналогичном периоде прошлого года совершено 633 киберпреступления. Наибольшее количество киберпреступлений зарегистрировано в Минском *(65)* и Борисовском *(51)* районах. Меньше всего зарегистрировано в Стародорожском *(2)* и Крупском *(1)* районах.

В структуре преступности преобладают хищения с использованием банковских платежных карт – 269 или 84,1% от общего количества зарегистрированных киберпреступлений. Оставшуюся часть сформировали киберпреступления, связанные с информационной безопасностью – 26, мошенничества и вымогательства – 25.

Абсолютное большинство преступлении данного вида совершено в отношении физических лиц, а основным способом совершения является хищение денежных средств с банковских счетов, характеризующиеся преобладанием мошеннических действий с использованием методов социальной инженерии (вишинг), в том числе с использованием различных торговых площадок, в целях завладения реквизитами банковских платежных карт или доступа к системам дистанционного банковского обслуживания (фишинг).

Справочно. Вишинг – метод несанкционированного доступа к информационным ресурсам, основанный на особенностях психологии человека. Фишинг – получение доступа к конфиденциальным данным, таким как адрес, телефон, номера банковских платежных карт, логины и пароли, путем использования поддельных веб-страниц ***(слайд №3)***.

Снижении количества регистрируемых киберпреступлений обусловлено проведением на постоянной основе профилактической работы с населением в рамках реализации плана мероприятий, направленных на принятие эффективных мер по противодействию киберпреступности, профилактике их совершения, повышения цифровой грамотности

населения на 2021 – 2022 годы, утвержденного 29.04.2021 заместителем председателя Минского облисполкома Маркевичем С.И.

Несмотря на положительные результаты профилактической работы, по-прежнему наиболее острой проблемой является беспечное отношение граждан к соблюдению базовых правила информационной безопасности.

Необходимо понимать, что безопасность в Интернете не имеет возрастных ограничений, поэтому каждый может защитить себя от киберпреступников не будучи экспертом. Все, что необходимо для обеспечения своей безопасности – это руководствоваться следующими правилами:

1. Не доверяйте позвонившим Вам незнакомым лицам.

Кибермошенники могут выдавать себя за кого угодно, например за представителя службы безопасности банка или сотрудника органов внутренних дел. Как правило, предлогом для звонка является обнаружение фактов несанкционированных денежных переводов с банковского счета за рубеж, которых на самом деле не было. Кроме того, часто используется мошенническая схема «оперативная игра». В ходе телефонной беседы в популярных мессенджерах жертве предлагается принять участие в оперативной игре по изобличению неблагонадежного сотрудника банка путем оформления кредита, который зачисляется на банковский счет. При этом могут использоваться поддельные служебные удостоверения сотрудников органов внутренних дел. Приведенные выше мошеннические схемы направлены не иначе как на хищение денежных средств под благовидным предлогом **(слайд №4)**.

Как Вы можете узнать, что Вас пытаются обмануть? Самый простой способ – это перестать общаться с незнакомцем и перезвонить в свой банк или в территориальный орган внутренних дел. Для этого достаточно набрать номер телефона круглосуточной службы поддержки клиентов банка, указанный на Вашей банковской платежной карте или номер 102, и в ходе телефонного разговора прояснить возникшую ситуацию.

Запомните, что ни при каких обстоятельствах нельзя сообщать (передавать) реквизиты банковских платежных карт (номер карты, срок действия, данные держателя, трехзначный код на обратной стороне карты), их фотографии, «логин» и «пароль» доступа к системе дистанционного банковского обслуживания «Интернет-банкинг» и коды доступа к нему в виде SMS-сообщений, поступающих из банка. Указанная информация является конфиденциальной и не подлежит разглашению даже представителям банка и сотрудникам правоохранительных органов. Если Вы не хотите получать звонки с незнакомых номеров, настройте в своем смартфоне защиту от лишних звонков **(слайд №5)**.

2. Безопасно посещайте сайты в сети Интернет.

Если Вы используете систему дистанционного банковского обслуживания «Интернет-банкинг» для расчетов за коммунальные услуги, денежных переводов, проверки факта зачисления на счет заработной платы (пенсий, пособий и т.п.), Вам необходимо удостовериться в подлинности веб-ссылки, предназначенной для авторизации на интернет-сайте банка.

Дело в том, что кибермошенники временно размещают в сети Интернет веб-ссылки, которые ведут на поддельные (фишинговые) веб-сайты, внешне не отличающиеся от оригинальных **(слайд №6)**.

В случае перехода на поддельный веб-сайт, Вам будет предложено ввести «логин» и «пароль» для авторизации. Если Вы это сделаете, то киберпреступники получат доступ к Вашему интернет-банкингу, а находящиеся на банковском счету денежные средства будут похищены **(слайд №7)**. Также Вам не следует переходить по ссылкам, которые Вы получили от неизвестных людей в социальных сетях или мессенджерах. С большой долей вероятности, данные ссылки являются фишинговыми.

Для безопасного совершения онлайн платежей рекомендуется использовать специальные приложения для мобильных устройств «Мобильный банкинг», которые доступны для скачивания в Google Play Market (для Android) или App Store (для iOS).

Распространенным примером фишинга являются всплывающие окна о каком-нибудь выигрыше денежном либо ином (айфон, автомобиль и т.д.). При нажатии на данное окно пользователь переходит по ссылке, где ему предлагается ввести свои личные данные, данные для входа в учетную запись социальной сети либо данные банковской платежной карты, которые в последствии достанутся злоумышленнику.

3. Исключите возможность компрометации реквизитов банковских платежных карт.

На поверхность банковской платежной карты нанесена информация о номере банковского счета, его владельце, сроке действия карты, трехзначный код (CVV-код). Этих данных достаточно, чтобы производить платежи за товары и услуги в сети Интернет. Утеря банковской платежной карты или ее временное нахождение, даже с Вашего согласия, в распоряжении посторонних лиц создают условия для компрометации ее реквизитов **(слайд №8)**.

Иногда бывает так, что банковскую платежную карту хранят в кошельке вместе с пин-кодом, записанным на ее поверхности или на листке бумаги. В случае утраты кошелька в результате утери или кражи, лицо им

завладевшее получает возможность полного доступа к Вашему банковскому счету.

Запомните, что нанесенная на поверхность банковской платежной карты информация является конфиденциальной и не подлежит разглашению посторонним лицам. Не храните Вашу банковскую платежную карту совместно с пин-кодом.

«Кардинг» – один из распространенных видов хищений денежных средств путем модификации компьютерной информации, направленный на завладение реквизитами банковских платежных карт с использованием специальных устройств, устанавливаемых на банкомат **(слайд №9-12)**.

Перед использованием банкомата необходимо убедиться в том, что на картоприемнике и клавиатуре не закреплены посторонние устройства. Рекомендуется прикрывать ладонью клавиатуру при вводе пин-кода, установить лимиты на максимальные суммы операций по снятию наличных, подключить смс-оповещение о проведении операций по карте.

5. Цифровая безопасность в сети Интернет (слайд №13).

Актуальной угрозой для пользователей сети Интернет являются компьютерные вирусы. Вирусы предназначены для нарушения работы компьютера, скрытого сбора данных о пользователе компьютера, таких как личных данных, паролей, документов, фотографий, размещенных в компьютере, для последующего вымогательства либо для передачи третьим лицам, так же для удаленного управления компьютером.

Не редко зараженные устройства будь это персональный компьютер, планшет или смартфон становятся частью «бот сети», позволяющей злоумышленнику выполнять противоправные действия с использованием ресурсов зараженного компьютера, который входит в сеть таких же зараженных компьютеров.

И так, что же может делать вирус на Вашем устройстве:

- собирать информацию о привычках пользования сетью Интернет и наиболее часто посещаемых сайтах;
- запоминать нажатия клавиш на клавиатуре, записывать скриншоты экрана и отправлять информацию создателю вируса;
- несанкционированно и удаленно управлять компьютером;
- устанавливать на компьютер дополнительные программы;
- изменять параметры операционной системы;
- перенаправлять на сайты, которые заражены другими вирусами.

Заразить устройство вирусом можно через нелицензионное (пиратское) программное обеспечение при его установке в операционную систему, при посещении сомнительных Интернет-ресурсов и скачивании

определенного контента, при открытии документов, вложенных в электронные письма, а также при переходе по ссылке для скачивания, которая указана в электронном письме.

Установите антивирус на все устройства. Предоставьте экспертам возможность заботиться о безопасности Вашего компьютера или смартфона, позволяя антивирусной программе присматривать за ними и защищать Ваши устройства от вредоносных программ. Антивирус поможет обеспечить безопасность при совершении онлайн-покупок и позволит Вам не беспокоиться при просмотре веб-сайтов.

Будьте осторожны с загрузкой вложений. Если Вы по электронной почте получили от неизвестного человека письмо с вложениями (как правило, это файлы с расширениями .zip, .rar, .exe, документ, медиа фалы ная фотография), никогда не открывайте их (не скачивайте). Такие вложения могут содержать вредоносные программы, которые могут инфицировать Ваш компьютер.

Не используйте одинаковые пароли для всех аккаунтов. Если Вы хотите зарегистрироваться на надежном и внушающем доверие сайте, обязательно используйте пароль, который сочетает в себе буквы, цифры и символы. Никогда не используйте одинаковый пароль для всех Ваших аккаунтов и регулярно меняйте их. Кроме того, не отправляйте Ваш пароль другим людям и не оставляйте его записанным где-либо.

6. Безопасность детей в сети Интернет.

Всем известно, что сеть Интернет предоставляет детям не только множество полезной информации и выбор развлечений, но и таит массу угроз, которые могут повлиять как на материальное состояние семьи, так и на психологическое здоровье детей.

На текущий момент возраст интернет-пользователя снизился настолько, что порой пятилетние малыши обращаются с компьютером и мобильными устройствами более ловко, чем взрослые. Поиск игр в сети Интернет, желание посмотреть фильм или мультфильм, по незнанию ребенка, а то и благодаря навязчивой рекламе, могут привести к попаданию на сайты, содержащие запрещенный контент.

Негативным для детей в интернет-пространстве также являются:

- кибербуллинг или троллинг – травля пользователя через все каналы сетевого общения: социальные сети, форумы, чаты, мессенджеры. Может принимать разные формы: оскорбления через личные сообщения, публикация и распространение конфиденциальной, провокационной информации о жертве. Проводить травлю могут как одноклассники, интернет-друзья и т.д., так и совершенно посторонние люди.

- информация, распространяемая в закрытых группах социальных сетей, провоцирующих детей на суицид, «игры на выживание» или «игры на вымирание», организованные создателями так называемых «групп смерти» (группы «Синий кит», «Беги или умри» и т.д.).

- незнакомцы в социальных сетях, за каждым из которых может стоять кто угодно.

Распространенным способом обеспечения безопасности детей в киберпространстве является использование программ родительского контроля, включающих в себя стандартный набор функций, а именно:

- *ограничение времени нахождения ребенка в сети;*
- *ограничение времени пользования компьютером;*
- *возможность создания графика с допустимыми часами работы в течение дня;*
- *блокировка сайтов с запрещенным контентом – создание «чёрных» списков на основе баз данных антивирусного производителя по категориям (наркотики, социальные сети и т.д.) и создание «белых списков» родителем;*
- *ограничение на запуск приложений (например, игр) и установку новых программ.*

Программы родительского контроля доступны для скачивания на официальных сайтах, в Google Play Market (для Android) или App Store (для iOS).

7. Рекомендации по безопасному использованию сети Интернет.

Для закрепления в памяти полученных Вами знаний, далее кратко приведены рекомендации по безопасному использованию сети Интернет:

- для выхода в сеть Интернет используйте устройства, на которых установлено антивирусное программное обеспечение;
- используйте операционную систему с установленными обновлениями безопасности;
- при использовании известных Вам сайтов, обращайте внимание на их внешний вид: возможно Вы зашли на поддельную его копию;
- не используйте одинаковые логины и пароли на различных сайтах;
- не используйте слишком легкие пароли, либо те, о которых можно легко догадаться;
- по возможности используйте двухфакторную аутентификацию, когда кроме ввода логина и пароля необходимо вводить временный код, отправляемый обычно на мобильный телефон в виде SMS-сообщения либо push-уведомления;

- остерегайтесь неожиданных или необычных электронных сообщений, даже если вам знаком отправитель, никогда не открывайте вложения и не переходите по ссылкам в таких сообщениях;

- при поступлении сообщений от знакомых, содержащих побуждение к осуществлению финансовых транзакций либо передаче финансовых реквизитов, обязательно необходимо проверить данную информацию с использованием других каналов связи;

- если Вы не используете банковскую платежную карточку для осуществления Интернет-платежей, обратитесь в банк для установки соответствующих ограничений для карты;

- при осуществлении Интернет-платежей по возможности используйте технологии обеспечения дополнительной безопасности платежей, такие как 3-D Secure для международных платежных систем Visa и MasterCard или Интернет пароль для платежной системы БЕЛКАРТ.

Управление по противодействию киберпреступности
криминальной милиции УВД Минского облисполкома