«КАК НЕ СТАТЬ ЖЕРТВОЙ В КИБЕРПРОСТРАНСТВЕ»
(*Материал предоставлен УВД Брестского облисполкома*)

СЛАЙД 1

Уже ни для кого не секрет, что вопросы обеспечения информационной безопасности в сети Интернет в настоящее время становятся все более актуальными. Информация и информационная технология все чаще выступают как предметом, так и средством совершения общественно опасных посягательств в информационной сфере. Практически все трудоспособное население, а также несовершеннолетние так или иначе вовлечены в процессы, связанные с ресурсами сети Интернет.

По данным Министерства связи и информатизации Республики Беларусь, на начало 2021 года услуги электросвязи в нашей стране оказывают 189 операторов. Количество абонентов стационарного широкополосного доступа в сеть интернет составляет 3,256 млн., количество абонентов сотовой связи составляет 11,66 млн и их количество постоянно растет. Преступность в сети Интернет приобретает все большие масштабы, изобретаются новые уловки, к которым наши граждане порой бывают не готовы, в том числе по причине минимальных познаний по обеспечению собственной информационной безопасности.

СЛАЙД 2

Состояние преступности в сфере высоких технологий

На протяжении последних лет число преступлений в сфере высоких технологий неуклонно продолжает расти. В 2020 году в Брестской области зарегистрировано 3124 высокотехнологичных преступлений (2019 - 1095, +185,3%).

Рост количества зарегистрированных преступлений по линии СВТ в основном обусловлен увеличением количества зарегистрированных хищений с использованием компьютерной техники (с 897 до 3053, +240,4%), из которых наиболее значительную часть составляют преступления, связанные с обращениями граждан по фактам хищений денежных средств с использованием полученных обманным путем реквизитов банковских платежных карт.

Как не стать жертвой хищений с использованием компьютерной техники

СЛАЙД 3

С 2020 года по настоящее время на территории Брестской области наблюдается всплеск активности преступлений, совершенных путем завладения реквизитами банковских карт в ходе телефонных разговоров

под видом сотрудника банка -«вишинг» и с помощью фишинговых страниц, имитирующих различные торговые интернет-площадки.

Справочно:

Вишинг *(англ. vishing, от voice phishing) — один из методов мошенничества с использованием социальной инженерии, который заключается в том, что злоумышленники, используя телефонную коммуникацию и играя определённую роль (сотрудника банка, покупателя и т. д.), под разными предлогами выманивают у держателя платежной карты конфиденциальную информацию или стимулируют к совершению определённых действий со своим карточным счетом / платежной картой.*

Фишинг *(англ. phishing от fishing «рыбная ловля, выуживание») — вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам, паролям и иной персональной информации. Это достигается путём проведения массовых рассылок электронных писем от имени различных организаций, а также личных сообщений внутри сервисов, например, от имени банков или посредством социальных сетей и мессенджеров. В письме зачастую содержится прямая ссылка на сайт, внешне неотличимый от настоящего, либо на сайт с редиректом (перенаправлением). После того как пользователь попадает на поддельную страницу, мошенники пытаются различными психологическими приёмами побудить пользователя ввести на поддельной странице свои логин и пароль, которые он использует для доступа к определённому сайту, реквизиты банковских платежных карт или иные персональные данные, что позволяет мошенникам получить доступ к аккаунтам и банковским счетам.*

В 2020 году с использованием методики «вишинга» злоумышленниками был совершено 988 (32% всех высокотехнологичных преступлений). По состоянию на 31.03.2021 года уже совершено 344 преступления данной категории (49% от всех зарегистрированных по линии СВТ в 2021 году). Злоумышленники, представляясь представителями банковских учреждений, осуществляют звонки на мобильные телефоны граждан и под видом представителя банковского учреждения Республики Беларусь пытаются завладеть реквизитами их банковских платежных карт и иными конфиденциальными данными. В процессе общения указанные лица сообщают, что необходимо срочно осуществить какие-либо действия с банковской платежной картой, так как кто-то либо пытается похитить с нее денежные средства, либо оформляет кредит или производит подозрительную оплату. В 2020 году для осуществления подобных звонков преступники зачастую использовали современные возможности сети Интернет, в частности возможность «подмены номера».

СЛАЙД 4

Суть «вишинга» заключается в том, что у потерпевшего на экране мобильного телефона отображается совершенно любой абонентский номер телефона, заданный злоумышленником, обычно это номер какого-либо банковского учреждения и сам звонок по своим внешним признакам не является подозрительным. В дальнейшем, предпринятыми ОВД определенными мерами, использование возможности «подмены номера» несколько утратило свою актуальность и в настоящее время для общения с гражданами преступники преимущественно используют различные интернет-мессенджеры, в частности «Viber», где в качестве имени пользователя (никнейма) они указывают официальный номер банка либо его название, в качестве «аватарки» используют логотип или эмблему банковского учреждения.

Следует отметить, что зачастую злоумышленники владеют какой-либо минимальной информацией о гражданах (имя, отчество, дата рождения, последние цифры банковской карты и др.), это способствует повышению доверия к звонящему и производит на него определенное впечатление. В дальнейшем злоумышленник просит сообщить информацию о банковской карте (ее номер, срок действия, CVV-код, содержание СМС-сообщения, которое в ходе разговора поступает на мобильный телефон). Получив интересующую информацию, он совершает хищение денежных средств. Существуют различные способы хищения денежных средств – путем перевода на иную банковскую карты, находящуюся в пользовании злоумышленника, электронные кошельки различных платежных систем, открытие онлайн-кредита и др.

В качестве примера изобретательности преступников можно привести следующий:

22 января 2021 года в УВД Брестского облисполкома поступило обращение жительницы г. Бреста по факту поступившего телефонного звонка от неустановленного лица с просьбой предоставления реквизитов банковской платежной карты. В ходе первоначальной проверки установлено, что 21.01.2021 в 12:09 часов на абонентский номер заявительницы в интернет мессенджере «Viber» поступил телефонный звонок от неизвестного ей ранее лица в никнейме которого был указан абонентский номер 375173375750 Звонивший мужчина представился сотрудником ОАО «БПС-Сбербанк» и настойчиво потребовал пригласить к телефону сына заявительницы 1982 г.р. Заявительница передала телефон своему сыну, которому неизвестный сообщил, что с находящейся у него банковской платежной карты происходит списание денежных средств и попросил предоставить персональные данные, чтобы заморозить транзакцию, на что последний ответил отказом, упомянув что не пользуется услугами ОАО «БПС-Сбербанк», а использует банковскую карту ОАО «Приорбанк» и положил трубку.

Через несколько минут с указанного выше абонентского номера поступил повторный звонок. Звонивший мужчина представился сотрудником ОАО «Приорбанк», повторно сообщил, что с находящейся у него банковской платежной карты происходит списание денежных средств и вновь попросил предоставить персональные данные и реквизиты находящейся в пользовании последнего банковской карты, на что вновь получил отказ. После указанного разговора на абонентский номер заявительницы в интернет мессенджере «Viber» поступил звонок с абонентского номера 37067876341 (указанный никнейм пользователя: «102»). Звонивший мужчина представился сотрудником ОВД Ленинского района г.Бреста майором милиции Соколовым Никитой Владимировичем и сообщил, что вышеуказанные звонки были осуществлены действительно от сотрудников банковских учреждений и попросил предоставить персональные данные ее сына, на что также получил отказ. Сразу же после окончания разговора с указанного выше номера поступил повторный звонок. Звонившая женщина представилась заведующей отделом финансов Московского района Никитиной Светланой и повторила просьбу о предоставлении ранее запрашиваемой информации, на что также получила отказ.

С целью предотвращения совершения преступлений указанной категории на территории области, сотрудниками ОВД во взаимодействии с иными правоохранительными органами, учреждениями образования, СМИ, трудовыми коллективами и иными заинтересованными проводится определенная профилактическая работа. К сожалению, следует констатировать факт, что имеются граждане, которые знали о подобного рода мошенничествах, вместе с тем попали на уловку так называемых «лжесотрудников» банков.

Следует обращать внимание на то, что **сотрудники банковских учреждений в телефонных разговорах никогда не уточняют у своих клиентов конфиденциальную информацию, а номер банковской платежной карты им всегда известен**.

СЛАЙД 5

Если Вам поступил такой звонок, **следует помнить**:

- **ни при каких обстоятельствах, никому и никогда не сообщайте информацию о себе или своей банковской платежной карте. Запомните, банк никогда не станет звонить своим клиентам посредством интернет-мессенджеров!** Если Вам будет звонить настоящий сотрудник банка, то он точно будет знать, как минимум номер Вашей банковской платежной карты и никогда не спросит конфиденциальную информацию в телефонном режиме. В случае если с использованием Вашего счета и правда кто-то будет пытаться совершить

несанкционированные операции и Банк это заметит, то его сотрудники сперва инициативно заблокируют Вашу банковскую платежную карту, после чего сообщат Вам причину принятого решения (ничего не уточняя) и пригласят в свое учреждения с паспортом для получения наличных денежных средств и написания заявления на перевыпуск карты;

- уточните с кем именно Вы общаетесь, после чего положите трубку и перезвоните на номер телефона, который отображался у Вас на экране (в этом случае Вы свяжитесь именно с тем абонентом, которому принадлежит указанный номер, а не со злоумышленниками, которые его использовали с целью скрыть свой настоящий номер) и уточните суть возникшей проблемы. Скорее всего собеседник сообщит, что Вам вообще не звонил. Современные технологии позволяют подменить номер на экране Вашего телефона на совершенно любой, в том числе заменить его для примера названием учреждения банка;

- если же на Вас оказывается психологическое давление угрозами, что через несколько секунд Вы понесете финансовые потери, кто-то оформит на Вас кредит или что если Вы не сообщите требуемую информацию, то карту вообще заблокируют, не волнуйтесь, это обычная уловка преступников, главная цель которых ввести Вас в состояние неуверенности и страха потерять сбережения. Даже в этом случае не сообщайте никакой информации собеседнику;

- сами перезвоните в свой банк или в круглосуточную службу сервиса, номер которой написан на оборотной стороне Вашей платежной карты и сообщите о случившемся. Скорее всего специалист сообщит Вам, что никаких несанкционированных операций зафиксировано не было, а сотрудник Банка Вам не звонил.

Если же Вы сообщили кому-либо информацию о своей банковской платежной карте, позвоните в свой Банк или примите иные меры к скорейшей ее блокировке. С заблокированного счета Вам без каких-либо затруднений и комиссий выдадут все денежные средства по предъявлению паспорта.

Помните, что если Вы сообщите злоумышленнику реквизиты своей банковской платежной карты, то он сможет распоряжаться всеми средствами на счету, а также оформить на Ваше имя дополнительные кредитные обязательства (онлайн-кредит).

В качестве примеров преступлений, совершенных с использованием методики «вишинга» можно привести следующие:

9 марта в 13.18 в РОВД обратилась Романюк Е.П., 1951 г.р., пенсионерка, жит. г. Бреста, что с 27 февраля по 6 марта неизвестный, находясь в неустановленном месте, путем телефонных звонков в мессенджере "Вайбер", от имени сотрудника ОАО "Белинвестбанк" с

просьбой предоставить рекивзиты банковской карточки и получив их похитил с карт-счета 59 850 рублей. ОСК ВУД по ч. 4 ст. 212 УК РБ.

26 марта ОСК ВУД по ч. 3 ст. 212 УК РБ по заявлению от 16 марта Просняк Г.К., 1965 г.р., медсестры УЗ "БГДБ", жит. г. Барановичи, что 15 марта с 16.00 до 19.00, неизвестный, находясь в неустановленном месте, путем телефонных звонков в мессенджере "Вайбер" от имени сотрудников ОАО "БПС-Сбербанк" с просьбой предоставить реквизиты банковской карточки и получив их, похитил с карт-счета 11214 рублей. Материал передан в ОСК 17 марта

31 марта в 16.50 в РОВД обратилась Черкас Т.А., 1971 г.р., заместитель заведующего Брестским филиалом ЧУО "Колледж бизнеса и права", жит. г. Бреста, что 31 марта в 14.30, неизвестный, находясь в неустановленном месте, с использованием глобальной сети "Интернет", путем телефонных звонков посредством мессенджера "Вайбер" от имени сотрудников ОАО "Банк БелВЭБ" с просьбой предоставить реквизиты банковской карточки и получив их, похитил с карт - счета 11850 рублей. ОСК ВУД по ч. 3 ст. 212 УК РБ.

Вторым наиболее распространенным способом преступлений указанной категории является «Фишинг» - получение злоумышленниками доступа к реквизитам банковских карт граждан с помощью фишинговых страниц, имитирующих различные торговые интернет-площадки. Таковых в прошедшем году совершено 1362 (44% всех высокотехнологичных преступлений). По состоянию на 31.03.2021 года уже совершено 255 преступлений данной категории (36% всех преступлений по линии СВТ, зарегистрированных в 2021 году).

В качестве примера торговой площадки, наиболее часто привлекающей злоумышленников, является «Куфар» (https://kufar.by) - популярный среди белорусов сайт объявлений, через который можно продавать и покупать вещи.

СЛАЙД 6

Сущность данного способа заключается в том, что преступник на какой-либо торговой площадке находит продавца, копирует его контактные данные, после чего ищет абонентский номер телефона продавца в различных интернет-мессенджерах, представляется покупателем и изъявляет желание приобрести товар по предоплате на Вашу карту. В дальнейшем он высылает продавцу фишинговую ссылку (ссылку на поддельную страницу) предоплаты, где продавцу необходимо ввести номер своей банковской карты для того, чтобы получить деньги от покупателя.

Поддельная страница визуально очень похожа на страницу реально существующей торговой площадки или вовсе идентична ей, размещают ее

на сайте, название которого визуально очень похоже на название сайта реальной площадки и имеет лишь незначительные различия, Естественно, никаких денег продавец не получит и как только он введет данные своей карты, они окажутся в руках мошенника, который получит доступ к карт-счету и сможет использовать размещенные на нем денежные средства по своему усмотрению. Актуальными являются схемы обмана покупателей и продавцов с использованием для доставки различных «фишинговых» почтовых сервисов (Европочта, Белпочта и др.)

СЛАЙД 7

Существуют и иные схемы «развода» как покупателей так и продавцов на различных торговых площадках. Их сущность заключается в том, чтобы получить реквизиты банковской карты с целью дальнейшего хищения денежных средств.

Наиболее оптимальным способом обезопасить себя будет открытие дополнительной банковской карты, которая будет предназначена лишь для совершения оплат в сети Интернет и на которой не будут хранится денежные средства.

СЛАЙД 8

Для того, чтобы не стать жертвой киберпреступников, совершая сделки в сети Интернет следует:

- вести общение с потенциальными покупателями или продавцами только во внутреннем чате торговой площадки (зачастую торговые площадки блокируют возможность перехода на поддельные ресурсы);
- ведя общение с пользователем стоит перейти к его профилю и обратить внимание на дату создания (если он создан несколько дней назад, то это должно вызвать дополнительную настороженность);
- очень внимательно относится к любому случаю, когда необходимо ввести данные карты или информацию, предоставленную банком (смс-код, логин или пароль от интернет-банкинга). Самый надежный способ уберечь свои средства – это никому не сообщать реквизиты своей карты;
- уточнить у собеседника номер телефона если он не указан в объявлении, а потом позвоните на этот номер, чтобы убедиться, что он реален и принадлежит именно пользователю, с которым вы совершаете сделку (очень часто злоумышленники используют номера телефонов, взятые в аренду на непродолжительное время и физического доступа к нему, не имеют);

-избегать перехода по неизвестным интернет-ссылкам, которые предоставляются в ходе переписки якобы для получения предоплаты или оформления доставки. Если Вам прислали такую ссылку, то, независимо от того, кто ее прислал, прежде чем по ней перейти, следует внимательно проверить доменное имя (адрес ресурса). Сделать это можно отыскав в

интернете официальный сайт и сверив написание доменного имени. Отличие в одну букву или символ свидетельствует о том, что перед Вами ссылка на поддельный ресурс.

СЛАЙД 9

Следует помнить **основные правила** информационной безопасности по защите банковской карты:

- Хранить в тайне пин-код, сведения с карточки сеансовых кодов;
- Прикрывать ладонью клавиатуру при вводе пин-кода;
- Оформить отдельную карту для онлайн-покупок, выезда за границу и не хранить на ней большие суммы. Для карты, используемой в РБ рекомендуется ограничить возможность ее использования за пределами РБ;
- Использовать двухфакторную аутентификацию, услугу «3-D Sequre», установить лимиты на максимальные суммы операций, подключить смс-оповещение о проведении операций по карте;
- Скрыть CVV (CVC) номер на карте (трехзначный номер на оборотной стороне), предварительно сохранив его;
- Подключить услугу «SMS-оповещение»;

Кроме того, вводить «логин» и «пароль» к системе «Интернет-банкинг» только на официальном сайте или в мобильном приложении банка. При обнаружении несанкционированного списания денежных средств с карт-счета, незамедлительно обратиться с заявлением в банк для их возврата по принципу «нулевой ответственности». Соблюдение этих несложных мер предосторожности позволит уберечь ваши денежные средства от преступных посягательств.

Если Вы все же ввели данные своей банковской карты на поддельном ресурсе или сообщили их постороннему лицу, необходимо в срочном порядке произвести блокировку карты, позвонив в банк либо самостоятельно в интернет-банкинге.

СЛАЙД 10

Видя проблему увеличения роста высокотехнологичных преступлений, в том числе совершенных с помощью методик «вишинга» и «фшинга», а также принимая во внимание минимальные познания населения по обеспечению собственной информационной безопасности в сети Интернет, Министерство внутренних дел Республики Беларусь постоянно разрабатывает материалы профилактической направленности. В качестве примера можно привести листовку на тему «Как не стать жертвой киберпреступника», в которой приведены шесть основных правил информационной безопасности, а именно:

- Надежные пароли;
- Безопасный WI-FI;

- Браузеры и сайты;
- Защита онлайн-банкинга;
- Использование приложений, соцсетей и мессенджеров;
- Безопасность электронной почты.

Как не стать жертвой преступлений в социальных сетях

На сегодняшний день в молодёжной среде мы вряд ли найдем кого-либо, кто не был бы зарегистрирован «ВКонтакте», «Фейсбуке», «Инстаграмм» каких-либо тематических форумах или иных площадках для виртуального общения. В целом это норма, ведь человек живет в обществе и стремится общаться. Однако некоторая неопытность, наивность и доверчивость порой приводит к негативным последствиям.

Основная проблема социальных сетей – это как раз доверие к тем, кто внесен в список «друзей». Бездумное предложение «дружбы» от неизвестных или малоизвестных людей может привести к драматическим последствиям.

Часто встречающаяся в настоящее время угроза – это взлом пользовательских учетных записей социальных ресурсов. Причин тому несколько и прежде всего – небрежное отношение пользователей к своим паролям.

Преступники прежде всего стремятся получить доступ к аккаунтам, которые защищенные простыми паролями. Для этого они запускают программы, подбирающие пароли и используют готовые словари и простые сочетания букв с цифрами.

Именно поэтому при создании пароля необходимо использовать комбинации букв, цифр, специальных символов, неочевидные ассоциации и сочетания различных элементов.

Стоит также помнить, что использовать один пароль для доступа к разным аккаунтам не рекомендуется так как каждый интернет-ресурс использует свои системы защиты и хранения паролей, которые не всегда могут быть реализованы на высоком уровне. Согласно статистике, около 14% пользователей используют один и тот же пароль для авторизации на всех аккаунтах и получив доступ к одному, злоумышленник непременно получит доступ и к другим. Стоит запомнить, что пароль — это секрет, который должен принадлежать только одному человеку, а если о нем знает кто-то еще, то это уже не секрет.

СЛАЙД 11

После совершения несанкционированного доступа к персональным аккаунтам, в течение первых суток зачастую развиваются следующие сценарии:

- злоумышленник, рассылает всем виртуальным «друзьям» потерпевшего просьбу под различными предлогами сообщить реквизиты банковской платежной карты. Это может быть ее фото или просто номер, срок действия и иные реквизиты, при этом, хоть в большинстве своем школьники банковских карт не имеют, но желая помочь «другу» очень часто используют карты своих родственников и друзей. Порой преступники просят просто номер мобильного телефона и либо пытаются похитить со счета телефона деньги или наоборот используют его как промежуточное звено, направляя на этот счет чужие деньги, переводя их затем дальше, чтобы запутать свои следы (практически во всех случаях хищения денежных средств со счетов мобильных телефонов потерпевшие еще сообщали преступнику персональные коды, приходящие в виде смс-сообщений на телефон).
- злоумышленник изучает содержание переписок потерпевшего и использует их содержание в качестве инструмента для вымогательства денежных средств. Таким образом, инструментом вымогательства становятся личные диалоги на откровенные темы, фотографии, содержащиеся на странице и в диалогах и иные очень личные данные. Обычно, перед тем как связаться с потерпевшим, преступник делает скриншот списка всех его друзей и близких. Избежать подобного возможно лишь путем регулярной чистки своих диалогов и удаления из сети всей информации компрометирующего характера.
- злоумышленник начинает рассылать различного рода порочащую информацию от имени владельца страницы иным пользователям, ссылки на поддельные ресурсы банковских учреждений, а также вредоносное программное обеспечение, что также может привести к серьезным последствиям.

В случае обнаружения «взлома» аккаунта, прежде всего, следует попытаться восстановить доступ наиболее привычным способом, путем отправки сообщения на «привязанный» номер мобильного телефона или электронную почту, кроме этого следует оповестить друзей и знакомых об инциденте, используя при этом иные социальные сети и мессенджеры. Кроме этого, чтобы в какой-то мере обезопасить себя от взлома, специалисты по безопасности рекомендуют «привязать» страницу социальной сети именно к номеру мобильного телефона, а не к адресу электронной почты, при этом вход на Вашу страницу с неизвестного компьютера или мобильного телефона будет не возможен без знания кода, который будет выслан на указанный при регистрации страницы номер.

Как не стать жертвой преступлений против информационной безопасности

СЛАЙД 12

К преступлениям против информационной безопасности относятся следующие уголовно-наказуемые деяния:

- Статья 349. Несанкционированный доступ к компьютерной информации;
- Статья 350. Модификация компьютерной информации;
- Статья 351. Компьютерный саботаж;
- Статья 352. Неправомерное завладение компьютерной информацией;
- Статья 353. Изготовление либо сбыт специальных средств для получения неправомерного доступа к компьютерной системе или сети;
- Статья 354. Разработка, использование либо распространение вредоносных программ;
- Статья 355. Нарушение правил эксплуатации компьютерной системы или сети.

Из преступлений указанной категории на территории области наиболее распространенными являются преступления, предусмотренные ст.354 УК Республики Беларусь (Разработка, использование либо распространение вредоносных программ).

С развитием сетевых технологий вредоносные программы получили новые возможности распространения и дополнительный, зачастую малозаметный пользователю функционал:

- вредоносное программное обеспечение может зашифровать данные на компьютере за расшифровку которых потребуют «выкуп».

- компьютер может начать работать медленно и со сбоями, потому что без вашего ведома его используют для атак на другие сайты или майнинга криптовалюты.

- у вас могут похитить личные данные, пароли от почтовых аккаунтов, страниц в социальных сетях.

- злоумышленники получат доступ к вашим платежным системам и личным кабинетам в банках. С ваших счетов будут сняты деньги, с помощью ваших карт расплатятся за чужие покупки в Интернете.

В ежедневном потоке сообщений злоумышленникам не составляет никакого труда спрятать вредоносные программы в электронных письмах, поступающий в ваши почтовые ящики, реальная цель которых не сообщить значимую информацию, а добыть ее у пользователя или вынудить совершить какие-либо действия. Стоит понимать, что любая информация, которой мы обмениваемся в Интернете, представляет потенциальную ценность если знать, как правильно ею воспользоваться.

Немаловажное значение в обеспечении безопасного использования электронной почты является внимательное отношение к содержимому входящей корреспонденции. Прикрепленные файлы обычно воспринимаются как рабочий инструмент и подозрения не вызывают.

Вследствие чего на расширение файла внимание обращается в последнюю очередь.

СЛАЙД 13

Чтобы не стать жертвой преступлений против информационной безопасности, следует неукоснительно следовать **правилам информационной безопасности:**

• не устанавливать программное обеспечение из неизвестных источников;

• не открывать электронных писем от неизвестных отправителей, не переходить по ссылкам и не запускать вложенные файлы;

• использовать наиболее современную версию антивирусного программного обеспечения;

• использовать безопасные (сложные) пароли, а также механизмы дополнительной аутентификации;

• хранить пароли в тайне даже от близких;

• не осуществлять переходов по подозрительным ссылкам и не вводить личную информацию (номера карт, телефонов и т.п.) ни под какими благовидными предлогами.

Используя электронную почту **всегда должны настораживать**:

- любые требования и просьбы сообщить пароль или иные персональные данные, поступившем даже от знакомого лица или якобы от представителя службы безопасности;

- любые письма с требованиями ввести или отправить свой пароль от онлайн-банка или реквизиты банковской платежной карты. Этими сведениями должен владеть только держатель карты и даже сотруднику банка их сообщать не стоит;

- всплывающие окна в том числе с предложениями поучаствовать в беспроигрышных акциях, а также письма с неоправданными пометками «Срочно!» и невнятно сформулированной темой письма. Помните: чем соблазнительнее предложение, тем выше вероятность того, что оно мошенническое.