Приложение к письму
Депинформтехнологий Югры
от «___»_____2023 г. № _____

Предложения
для формирования методических рекомендаций для граждан старшего поколения по противодействию мошенничеству в информационной среде, включая мошенничество с пластиковыми картами и вредоносными программами в сети «Интернет».

Основные способы мошенников при выманивании личных данных и средств:	Практические рекомендации, как избежать угрозы в Интернете. Основные способы защиты от мошеннических действий и вредоносных программ:
Фишинг (мошеннические веб-сайты, веб-ресурсы, полностью имитирующие ресурсы известных банков, платежных систем или других ведомств или имитирующие веб-ресурсы организаций, которым пользователь/держатель карты доверяет для выманивание у пользователей персональных, финансовых или конфиденциальных данных под видом предоставления несуществующих услуг в целях хищения и использования этой информации и данных в мошеннических целях. Мошеннические веб-сайты, веб-ресурсы могут быть похожи на письма, которые приходят из банков или других официальных органов и организаций; могут быть рассылки в социальных сетях от якобы знакомых или друзей; мошенники могут использовать актуальные новости для создания поддельных веб-сайтов.	***Смотрите, что Вы скачиваете*** (файлы должны быть загружены только из доверенных источников) ***Используйте сложные пароли, чтобы сделать их надежными*** (длинные пароли и комбинации чисел, букв и символов) ***Используйте менеджер паролей*** (менеджеры паролей помогут Вам хранить пароли безопасными и уникальными для каждого веб-сайта) ***Регулярно меняйте свои пароли*** (убедитесь, что Ваш пароль надежный и не повторяется на других веб-сайтах и) ***Не доверяйте незапрашиваемым сообщениям, не отвечайте на подозрительные электронные письма и смс-сообщения*** (не переходите и не кликайте на ссылки, указанные в подозрительных сообщениях, не подписывайтесь на сомнительные веб-сайты в электронных письмах, не устанавливайте приложения по просьбе якобы сотрудников банков) ***Не пользуйтесь услугами непроверенных и неизвестных сайтов*** (не открывайте файлы или ссылки, полученные из ненадежных источников) ***Чтобы распознать фишинговый сайт, необходимо обратить внимание на:*** - отсутствие безопасного соединения https:// (адрес веб-страницы начинается с https://); - отсутствие зеленого замка, оповещающего об установке защищенного https://соединения; - сайт зарегистрирован на домене, где не существует ограничений для регистрации (например: .ru, .com, .org, .net, .info, .biz, .top, .in, .cc, .com.ua, .in.ua, .pp.ua, .kiev.ua, .dp.ua, .te.ua) или используется домен конструктора сайтов (например: Jimdo,Heroku); - в адресной строке высвечивается одинаковый адрес для всех страниц сайта;

	- отсутствие авторизационного запроса по карточке (в случае обращения держателя карты в свой банк – банк не подтверждает проведение или попытку проведения операции на указанном сайте); - грамматические, стилистические синтаксические ошибки и опечатки в текстовках сайта
Поддельные звонки (мошенники звонят по телефону и заставляют Вас поделиться личной/ конфиденциальной информацией, заявляя, что необходима помощь в решении проблемы. Мошенники могут использовать социальный контакт,социальные медиа, чтобы получить вашу личную информацию)	***Не передавайте личные данные по телефону:*** - не сообщайте посторонним людям конфиденциальную информацию и персональные данные (паспортные данные, дата и место рождения, семейное положение, образование – они считаются конфиденциальными если владелец не давал разрешения на их публичное представление в СМИ или Интернете); - никогда не размещайте в открытом доступе информацию личного характера; не публикуйте информацию о себе в социальных сетях, на форумах и каких-либо сайтах в Интернете; помните, что видео и аудиотрансляции и Ваша переписка могут быть сохранены злоумышленниками, и впоследствии использована против Вас; - при получении смс-сообщений, содержащих информацию о том, что Ваша банковская карта заблокирована в силу ряда причин не звоните и не отправляйте ответного сообщения на номер, с которого оно пришло или номера, указанные в смс-уведомлении, не отправляйте никаких денежных средств по координатам, указанным в смс; - не совершайте каких-либо действий по счету, если вам звонят с просьбой или требованием о переводе денег, в том числе на «защищенный» или «специальный» счет Центробанка, или с предложением об оформлении кредита (банк России не открывает счета и не работает с гражданами); - при поступлении звонка от якобы сотрудника банка или представителя любых других организаций с просьбой установить приложение для удаленного доступа на Ваше устройство с интернет-банкингом – немедленно прервите разговор, не устанавливайте никаких приложений, не сообщайте реквизиты, логины и пароли, SMS-коды, «сеансовые ключи» или одноразовые пароли 3-D Secure, полученные Вами в смс-сообщении, системах дистанционного банковского обслуживания; - запомните, что банки никогда не запрашивают Ваши пароли по телефону
Вредоносные программы (программное обеспечение, которое может украсть Ваши данные или повредить Ваш компьютер) <u>Виды вредоносных программ:</u>	***Установите антивирусное программное обеспечение*** (защитите свой компьютер от кражи данных и вредоносных программ. Помните, что установка антивирусного программного обеспечения на Ваш персональный компьютер или

- вирусы (замедляют работу компьютера, могут удалять файлы или перехватывать Вашу конфиденциальную информацию); - файлы-шпионы (программное обеспечение, которое может отслеживать Ваши активности на компьютере и сообщать мошенникам); - рекламные вредоносные программы (рекламы, которые содержат вредоносный код, который может украсть Ваши данные)	на мобильное устройство – это не прихоть, а мера позволяющая повысить вашу безопасность) ***Обновляйте антивирусное программное обеспечение*** (большинство обновлений программного обеспечения предназначено для устранения уязвимостей безопасности) ***Используйте технические средства защиты*** (например, фильтры входящих звонков и т.п.) ***Регулярно обновляйте*** приложения, операционную систему и защитные решения (сигнатуры) ***Работайте только на защищенном персональном компьютере*** (с ограниченным физическим доступом к нему посторонних лиц)
Клонирование банковских карт или банковских счетов (позволяет мошенникам не просто совершать разовые несанкционированные транзакции или похищать личные данные, но и создавать точную копию карты, пригодную для многократного совершения платежей)	***Проявляйте внимательность и аккуратность при использовании карты:*** - бережно храните пластиковые карты, их нельзя мочить, хранить рядом с мобильным телефоном, офисной и домашней техникой; - не храните данные карт и PIN-коды на компьютере или в смартфоне; - не отдавайте банковскую карту продавцам, официантам, обслуживающему персоналу и не оставляйте ее без присмотра; - следите, чтобы никто не видел, как Вы вводите пин-код карты; - не сообщайте посторонним людям финансовые сведения, реквизиты банковских карт, личные данные, трех-значный код с обратной стороны карт или СМС-код; - если при оплате пластиковой картой произошла ошибка, не выбрасывайте чек, который выдал терминал, проверьте, была ли произведена операция. ***Используйте проверенные банкоматы и терминалы:*** - не пользуйтесь банкоматами, которые долго находятся в режиме ожидания, часто перезагружаются или Вы видите на экране подозрительные изображения, а вокруг карто-приемника подозрительные материалы (следы клея, провода и др.) – это признаки некорректной работы, сообщите об этом в банк по телефону, указанному на банкомате; - внимательно осматривайте банкомат перед тем, как им воспользоваться – на клавиатуре и картридере не должно быть никаких дополнительных приспособлений (подозрения должны вызывать отличия в цветах между смежными элементами, щели и зазоры, люфты у кардридера или клавиатуры); - для защиты карт от копирования многие современные банкоматы имеют специальные

	механизмы, например, прозрачный кардридер, в котором будет просто заметить постороннее устройство, а для защиты банковской карты от считывания по воздуху используются специальные чехлы, кошельки, карт-холдеры. ***Для безопасного использования банковских карт соблюдайте следующие меры:*** - для повышения безопасности расчетов в сети Интернет заведите отдельную карту для совершения операций через сеть Интернет; - подключите услугу дополнительной аутентификации держателя карты «3-D Secure»; - пользуйтесь интернет-банком и мобильным банком только с личных устройств, проверяйте свой счет и статус баланса банковской карты через мобильное приложение или онлайн-банкинг, отслеживайте свои транзакции; - установите сумму месячного лимита и подключите смс-оповещение о всех снимаемых средствах; - проверяйте наименование сайта при переходе на страницу для ввода реквизитов банковской карточки; - не заходите в интернет-банк и мобильный банк через открытые сети Wi-Fi; - скачивайте приложения для проведения платежей только из официальных магазинов (Google Play Store, AppStore) и официальных сайтов банков; - не вводите данные карточки (номер, дату окончания срока действия, коды защиты CVV2/CVC2) на веб-сайтах, предлагающих вознаграждения на платежную карту, а также на других подозрительных сайтах; - если Вы потеряли карту, немедленно заблокируйте её через мобильное приложение и обратитесь в банк, который выдавал карту (если этого не сделать, банк не будет нести ответственность за списанные средства); - пересчитывайте денежные средства после получения наличности в банкомате и не забывайте забирать карту; - никогда не перечисляйте деньги не знакомым лицам на их электронные счета, электронные кошельки и счета мобильных телефонов