Безопасность расчетов в сети Интернет
с использованием банковской платежной карточки

Интернет ”шагает“ по планете семимильными шагами. В современном мире это не только информационный ресурс, но и посредник между потребителями и поставщиками товаров и услуг.

Сегодня, не выходя из дома, в сетях Интернета возможно осуществлять любые платежи, открывать вклады, перечислять деньги, оплачивать услуги и товары. Причем совершать покупки можно в интернет-магазинах всего мира. Достаточно иметь платежную карту – реальную или виртуальную. Но как же самому не попасться в эти сети, проводя шопинг по страницам интернет-магазинов?

Для повышения безопасности расчетов в сети Интернет и расширения возможности контроля таких расчетов рекомендуется следующее:

✓ Приобретите отдельную карточку для совершения операций в сети Интернет.

✓ Не храните на счете, к которому выпущена карточка, для осуществления покупок в Интернете, крупные суммы денег. Пополняйте счет непосредственно перед оплатой, желательно на сумму, необходимую для совершения покупки. По возможности блокируйте карточку после проведения операции.

✓ Выбирайте сложные, символьно-цифровые пароли, которые не связаны с днем рождения или другими персональными данными. Не записывайте пароли и никому не сообщайте их.

✓ Не сообщайте свой ПИН-код при заказе товаров на сайте торговой точки. ***Помните! При совершении удаленных операций ввод ПИН-кода никогда не требуется.***

✓ Обязательно подключите услугу дополнительной аутентификации* держателя карточки 3-D Secure.

**Аутентификация — процедура проверки подлинности. Аутентификация требуется при доступе к таким интернет-сервисам как: электронная почта, веб-форум, социальные сети, интернет-банкинг, платежные системы, корпоративные сайты, интернет-магазины.* При совершении операций через интернет-сайты, которые сертифицированы международными платежными системами Visa International и MasterCard Worldwide на технологию 3-D Secure, необходимо ввести одноразовый пароль, который предоставляется в виде

SMS-сообщения на номер мобильного телефона или в системах дистанционного банковского обслуживания. Сертифицированные интернет-сайты определяются по наличию следующих логотипов:

✓ Не сообщайте никому персональные данные, а также сеансовые ключи или одноразовый пароль 3-D Secure, полученный Вами в SMS-сообщении, системах дистанционного банковского обслуживания. Данные пароли можно использовать только для подтверждения операции в сети Интернет, которая проводится непосредственно Вами.

✓ Обязательно сообщите банку-эмитенту (то есть банку, выдавшему карточку) об изменении Вашего номера мобильного телефона, который был указан при подключении услуги 3-D Secure, а также о фактах утери мобильного устройства и (или) SIM-карты.

✓ Совершайте покупки только со своего личного компьютера. Это позволит сохранить конфиденциальность персональных данных. Если же все-таки покупка совершена с чужого компьютера, – не сохраняйте на нем персональные данные и информацию о платежной карте и счете, а также убедитесь, что они не сохранились автоматически. Для этого вновь загрузите в браузере* web-страницу продавца, на которой совершались покупки. Используйте последние версии браузеров.

**Бра́узер, или веб-обозреватель (англ. web browser) — прикладное программное обеспечение для просмотра веб-страниц, содержания веб-документов, компьютерных файлов и их каталогов; управления веб-приложениями. В глобальной сети браузеры используют для запроса, обработки, манипулирования и отображения содержания веб-сайтов.*

✓ Установите на свой компьютер антивирусное программное обеспечение и регулярно производите его обновление и обновление других используемых программных продуктов (операционной системы и прикладных программ). Это защитит от вирусов и других деструктивных программ.

✓ Не заходите в интернет-банк через открытые сети Wi-Fi.

✓ Пользуйтесь интернет-сайтами только известных и проверенных организаций торговли и услуг. Внимательно читайте условия договора о предоставлении услуг на интернет-сайтах, особенно по операциям, связанным с азартными играми: казино, лотереи.

✓ Обязательно убеждайтесь в правильности адресов интернет-сайтов, на которых собираетесь совершить покупки, поскольку похожие адреса могут использоваться для осуществления неправомерных действий.

✓ Проверяйте наименование сайта при переходе на страницу для ввода реквизитов карточки.

Важно также определить, не является ли сайт, который вы хотите посетить, фишинговым*.

**Так называемый "фишинговый сайт" – это веб-ресурс, выманивающий реквизиты банковских платежных карточек с целью хищения и использования конфиденциальной информации в мошеннических целях. Происходит это под видом предоставления несуществующих услуг или имитации веб-ресурса организации, которому держатель доверяет.*

Чтобы случайно не раскрыть данные своей карточки мошенникам, следует обратить внимание на следующие условия:

✓ отсутствует безопасное соединение по протоколу HTTPS, – адрес веб-страницы начинается с http:// и не имеет зеленого замка, оповещающего об установке защищённого 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);

**Домен — это адрес созданного сайта или определенная зона, которая имеет свое имя, не похожее ни на одно другое в системе доменных имен.*

✓ сайт расположен на веб-сервере в другом государстве, например, веб-сайт платежного сервиса России или Украины расположен в Германии, США, Латвии, Китае, Перу, Зимбабве;

✓ сайт зарегистрирован недавно и оплачен на короткий срок (например, 1 год);

✓ грамматические, стилистические, синтаксические ошибки и опечатки в текстовках сайта;

✓ слишком хорошо, чтобы быть правдой;

✓ после введения реквизитов карточки держатель получает сообщение об отказе в проведении операции (например, "Операция отменена банком! Возможные причины: …"), реже – сообщение об успешной операции, но при этом оплаченные услуги держателю не предоставляются;

✓ в случае обращения держателя в свой банк, банк не подтверждает проведение или попытку проведения операции на указанном сайте, авторизационный запрос по карточке отсутствует;

✓ в адресной строке высвечивается одинаковый адрес для всех страниц сайта;

✓ наличие "нестыковок" в текстовках сайта – даты сообщений и новостей неактуальные, информация в футере* и хедере** сайта не соответствует основному тексту (например, название сайта на баннере*** и футере сайта не соответствует названию сайта в адресной строке).

**Футер (англ. footer, подвал) – это блок в нижней части страницы, куда выносят полезную, но не первостепенную информацию.*

***Хедер (англ. header, шапка) – это блок в верхней части страницы сайта, в котором, как правило, размещается логотип и слоган сайта, краткая контактная информация, основное горизонтальное меню и другие элементы, которые считаются наиболее важными в зависимости от специфики ресурса.*

****Баннер (англ. Banner, флаг, транспарант) — графическое изображение рекламного характера.*

Придерживаясь указанных правил, вы снизите риски и не окажетесь жертвой мошенников в сети Интернет, а ваш шопинг будет удачным и не превратиться в обременительные разбирательства и денежные потери.

Главное управление Национального банка
Республики Беларусь по Могилевской области