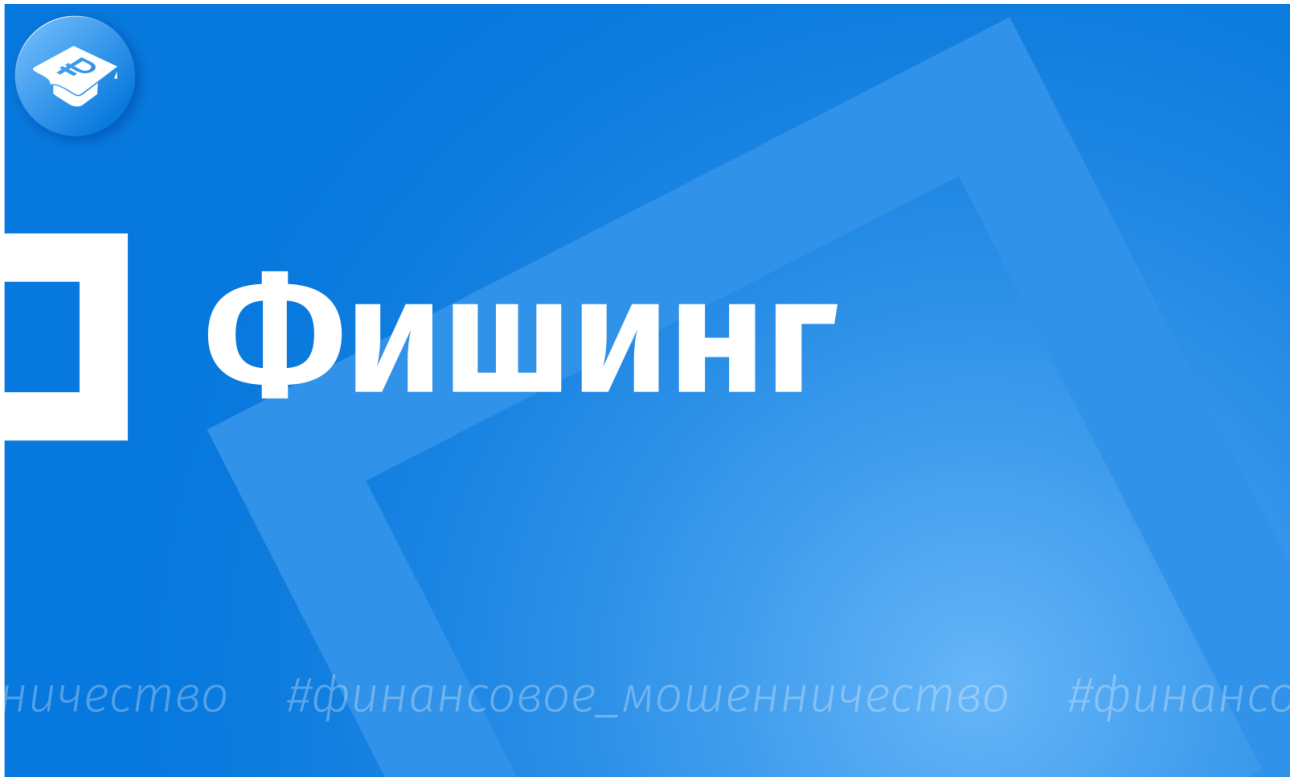
24 МАРТА, ПЯТНИЦА

Открытый бюджет города Москвы

Что такое фишинг, и какие приемы используют мошенники



Фишинг – то есть рыбалка, ловля на крючок, вид интернет-мошенничества с целью хищения конфиденциальной информации граждан (сведений о банковских картах, паролей, учетных записей и иных персональных данных) путем рассылки электронных писем, смс-уведомлений, сообщений в мессенджерах или социальных сетях с вредоносными ссылками, переход по которым, как правило, грозит утечкой личных данных и потерей денежных средств.

Мошенники используют следующие приемы фишинга:

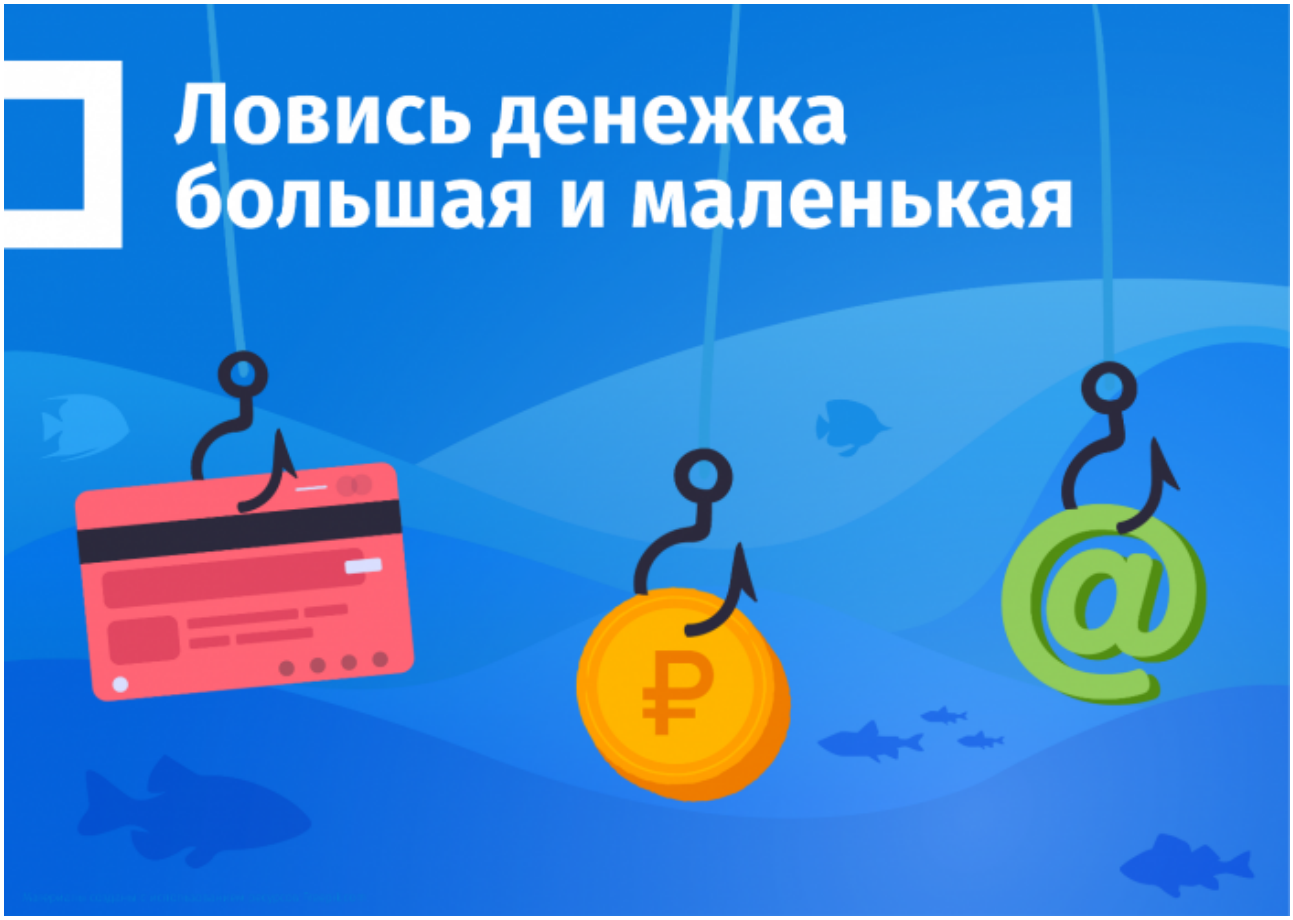
- **Сообщают о выгодных скидках, крупном выигрыше или неожиданном поступлении на ваш банковский счет денежных средств.** Для получения подробной информации злоумышленники предлагают перейти по ссылке в письме или сообщении и ввести персональные данные в специальную форму. Такие действия могут привести к их утечке или хищению денежных средств со счета;
- **Направляют в мессенджерах и социальных сетях сообщения от имени друзей или близких.** Мошенники взламывают страницу пользователя или создают ее аналог и распространяют сообщения с предложением получить подарок, выгодно и быстро заработать, проголосовать за участника конкурса или срочно перечислить денежные средства в связи с экстренной жизненной ситуацией;

- **Рассылают письма и сообщения от имени государственных органов.** Злоумышленники рассылают ложные уведомления о назначении и выплате социальных пособий, предлагают перейти по ссылке и ввести данные банковской карты для их перечисления гражданину;
- **Подделывают сайты действующих интернет-магазинов.** Кибермошенники копируют структуру и интерфейс официальных страниц торговых площадок, формируют похожий URL-адрес (адрес сайта или его страниц), отличающийся на 1-2 символа. Затем от имени представителя компании направляют в сообщении ссылку на фишинговый сайт для оплаты или перевода денежных средств. С аналогичным приемом фишинга можно столкнуться при оплате услуг мобильной связи, ЖКХ, налогов или госпошлин;
- **Передают вредоносные программы под видом обновления ПО.** Мошенники, направляя сообщения по электронной почте или через мессенджеры, предлагают загрузить новое приложение или установить обновление с помощью «специальной программы». Скачанные файлы зачастую содержат вирусы, которые могут нарушить работу устройств и предоставить злоумышленникам доступ к конфиденциальным данным;
- **Используют вредоносные QR-коды.** Мошенники создают их для перехода на фишинговые сайты, размещают на рекламных буклетах, остановках, парковках, в общественных местах и других объектах массового скопления людей;
- **Предлагают применять VPN-сервисы**. Злоумышленники распространяют в сети Интернет программы и приложения, влекущие нарушение системы защиты устройства, под видом VPN-сервисов. Устанавливая их на компьютер или смартфон, пользователь предоставляет кибермошеннику доступ к своим персональным данным.

Как защититься от фишинга:

- Внимательно проверяйте адреса сайтов. Символ закрытого замка и https:// в адресной строке означают защищенное соединение. Фишинговый сайт может отличаться от настоящего лишь несколькими символами. Проверить безопасность ресурса можно с помощью специальных сервисов поисковых систем, а адрес страницы финансовой организации – в онлайн-реестре на сайте Банка России. Сайты крупных банков и государственных органов в российских поисковых системах отмечены специальным значком – цветным кружком с галочкой. Проверенные адреса можно сохранить в закладках браузера для последующего использования;
- Не открывайте сомнительные ссылки, если в теме сообщения указана информация о выплатах, выигрышах в лотереях и конкурсах, не загружайте файлы и приложения. Если вам знаком автор сообщения или письма, перезвоните ему и убедитесь в достоверности полученной информации;
- Установите на устройства антивирусное программное обеспечение, оно обезопасит вас от поддельных веб-сайтов и спам-сообщений;

Используйте отдельную карту для покупок в сети Интернет и пополняйте её непосредственно перед оплатой. Не совершайте предоплату товара или услуги на непроверенных сайтах.



По материалам портала Правительства Москвы "Открытый бюджет города Москвы":
https://budget.mos.ru/