Для немедленной публикации: 22.03.2022 **ГУБЕРНАТОР КЭТИ ХОКУЛ**

ГУБЕРНАТОР ХОКУЛ ПРЕДУПРЕДИЛА ЖИТЕЛЕЙ О МОШЕННИЧЕСТВЕ И УГРОЗАХ КИБЕРБЕЗОПАСНОСТИ НА ФОНЕ ВТОРЖЕНИЯ РОССИИ В УКРАИНУ

Губернатор призывает жертвовать средства только проверенным и авторитетным организациям, которые используют пожертвования для оказания помощи нуждающимся украинцам

Ведомства штата издают рекомендации по защите и обеспечению безопасности вашей чувствительной информации сохранению бдительности в условиях повышенного риска киберугроз

Сегодня Губернатор Кэти Хокул предупредила жителей Нью-Йорка о случаях мошенничества в сфере благотворительности и возросших угрозах кибербезопасности, связанных с вторжением Владимира Путина в Украину. Управление по защите прав потребителей штата Нью-Йорк выявило случаи мошенничества с просьбами о выделении денег на благотворительность для поддержки жертв войны. Мы рекомендуем жителям тщательно оценивать любые просьбы о деньгах и проверять благотворительные организации, прежде чем жертвовать деньги или материальные средства. Губернатор Хокул также призывает жителей Нью-Йорка сохранять бдительность при раскрытии конфиденциальной информации в Интернете на фоне роста угроз кибербезопасности, используя рекомендации по безопасности от Департамента налогообложения и финансов (Department of Taxation and Finance). Это произошло после того, как губернатор сформировала Объединенный оперативный центр обеспечения безопасности (Joint Security Operations Center, JSOC), который служит центром для совместно реализуемой деятельности местных властей, властей штата и федерального правительства в сфере кибербезопасности.

«В Нью-Йорке проживает самое большое число украинцев в США, и жители Нью-Йорка всегда протягивают руку помощи, заботясь о тех, кто в ней нуждается, — **сказала губернатор Хокул.** — «Однако мы должны сохранять бдительность по отношению к тем, кто пытается совершить мошенничество, пользуясь добротой других людей. В своем стремлении помочь нашим украинским друзьям и близким помните, что если что-то кажется подозрительным, то, скорее всего, так оно и

есть. Призывайте своих друзей и родственников, особенно пожилых людей, быть бдительными в Интернете».

При любых чрезвычайных ситуациях мошенники пытаются играть на чувствах людей, желающих помочь. Вторжение в Украину дает мошенникам возможность создавать фальшивые благотворительные организации или выдавать себя за убедительных жертв войны. Другие создают веб-сайты, имитирующие официальный сайт законной благотворительной организации, чтобы украсть деньги и личную информацию ничего не подозревающих жертвователей.

Секретарь штата Роберт Дж. Родригес: «Жители Нью-Йорка известны своей поддержкой и отзывчивостью по отношению к нуждающимся. Пока в Украине продолжается война, будут продолжать появляться мошенники, пользующиеся эмоциональными уловками и ложными призывами в попытке обмануть людей. Я призываю жителей Нью-Йорка защищать свои добрые намерения и всегда проверять благотворительные организации, прежде чем сделать пожертвование, чтобы ваши с трудом заработанные доллары попали именно к тем, кто так отчаянно нуждается в вашей поддержке».

Исполняющая обязанности начальника Департамента налогов и финансов Аманда Хиллер (Amanda Hiller): «Глобальный кризис в Украине усилил беспокойство по поводу кибератак, поэтому мы все должны быть бдительными, чтобы предотвратить попадание конфиденциальной информации в чужие руки, DOS атаки и другие негативные последствия».

Генеральный директор Бюро штата Нью-Йорк по информационно-техническому обслуживанию (New York State Office of Information Technology Services) Тони Риддик (Tony Riddick): «Бесчисленное количество жителей Нью-Йорка с самыми добрыми намерениями жертвуют в благотворительные фонды в поддержку народа Украины, и это действительно имеет огромное значение. К сожалению, такая отзывчивость также создает новые возможности для киберпреступников. Чтобы защитить себя и гарантировать, что ваше щедрое пожертвование точно попадет в руки тех, кто действительно нуждается в помощи, Бюро ITS просит жителей Нью-Йорка следовать рекомендациям и сохранять бдительность в свете недавних онлайн-угроз и кибер-мошенничества».

Руководитель Управления по вопросам национальной безопасности и чрезвычайных ситуаций (Division of Homeland Security and Emergency Services) Джеки Брей (Jackie Bray): «Каждый житель Нью-Йорка должен сыграть свою роль в обеспечении безопасности своей личной информации и защите от киберугроз. Мы знаем, что в трудные времена недобросовестные люди пытаются воспользоваться теми, кто пытается помочь. Если вы пытаетесь поддержать народ Украины через онлайн или цифровые пожертвования, будьте бдительны и следуйте этим рекомендациям, чтобы обеспечить надежность ваших пожертвований и безопасность вашей информации».

Сенатор штата Кевин Томас (Kevin Thomas): «То, что так много жителей Нью-Йорка приняли меры для помощи украинскому народу, говорит о многом. К сожалению, этот кризис также создал прекрасную возможность для мошенников использовать его в своих корыстных целях. Я призываю жителей Нью-Йорка сохранять бдительность и принимать дополнительные меры предосторожности, чтобы убедиться, что их честные пожертвования идут на законные цели».

Член Ассамблеи Нили Розич (Nily Rozic): «Мошенники постоянно прибегают к новым способам обмануть вас, даже во время международного кризиса. В то время как жители Нью-Йорка собираются вместе, чтобы поддержать Украину в трудную минуту, очень важно, чтобы они были вооружены навыками и знаниями для того, чтобы их щедростью не воспользовались. Я благодарна губернатору Хокул за то, что она заботится о том, чтобы жители Нью-Йорка не были обмануты в своей доброте».

Мошенники часто связываются с людьми через социальные сети, незапрошенные электронные письма, телефонные звонки или текстовые сообщения. Они могут попросить отправить деньги через платежное приложение, такое как Cash App, Venmo или Zelle, перевести деньги на счет в оффшорном банке или отправить предоплаченные подарочные карты. Многие последние мошенничества также содержали просьбы о пожертвованиях в криптовалюте, такой как Bitcoin или Ethereum. Аферисты изобретательны и будут продолжать придумывать новые способы обмана людей, поэтому жители всегда должны оставаться бдительными.

Чтобы предотвратить попадание пожертвованных средств в чужие руки, Отдел по защите прав потребителей штата Нью-Йорк рекомендует принять следующие меры предосторожности:

- **Проверьте запрос.** Мошенники все чаще выдают себя за друзей, родственников или романтических партнеров в социальных сетях и просят сделать пожертвование; скопировать чужую фотографию и биографические данные и создать фальшивый аккаунт в Интернете очень просто. Если вы получили нежелательную просьбу об оказании помощи в виде пожертвований через Интернет, даже если это кажется знакомый вам человек, свяжитесь с ним напрямую через другой канал связи, чтобы проверить просьбу. Не переходите по ссылкам и не заполняйте формы до проверки источника. Если просьба исходит от человека, с которым вы недавно познакомились в Интернете, скорее всего, это мошенничество, и вам следует быть особенно осторожными.
- **Изучите благотворительную организацию** Не полагайтесь только на веб-сайт благотворительной организации. Прежде чем жертвовать в какую-либо благотворительную организацию, поищите информацию о ней в Интернете, используя название организации и такие поисковые запросы, как «отзывы» и «мошенничество». Федеральная торговая комиссия (Federal Trade Commission) рекомендует посетить сайты give.org, charitynavigator.org,

charitywatch.org или candid.org и ознакомиться с отчетами и рейтингами благотворительных организаций. Вы также можете обратиться в Налоговое управление (the Internal Revenue Service, IRS) для проверки того, зарегистрирована ли благотворительная организация. Генеральная прокуратура также рекомендует проверять реестр благотворительных организаций (Charities Registry) на предмет наличия финансовых отчетов до внесения пожертвований, чтобы убедиться в финансовой состоятельности благотворительной организации.

- **Не поддавайтесь тактике высокого давления.** Хотя ситуация не терпит отлагательств, не поддавайтесь давлению немедленно сделать пожертвование. Мошенники часто вынуждают вас немедленно пожертвовать деньги, не обращая внимания на тревожные сигналы в их истории. Остерегайтесь прямых электронных писем от «жертв» и просителей, которые рассказывают душераздирающие истории, настаивая на том, чтобы вы немедленно сделали пожертвование. Не передавайте деньги по телефону нежелательным телемаркетологам; вместо этого попросите звонящего прислать письменные материалы о благотворительной организации и о том, куда можно пожертвовать, если вы решите это сделать.
- **Храните личную информацию в закрытом доступе.** Никогда не сообщайте номер социального страхования, номер кредитной или дебетовой карты или другую личную идентификационную информацию в ответ на непрошеную просьбу о благотворительности. Если вы жертвуете через Интернет, прежде чем выполнять просьбы о пожертвовании, убедитесь, что ваше интернет-соединение надежно.
- **Узнайте, как будут потрачены ваши деньги.** Убедитесь, что ваши деньги идут непосредственно пострадавшим. Настоящая благотворительная организация должна быть в состоянии сообщить вам, какая часть вашего пожертвования пойдет непосредственно на программу, а не на административные расходы.

- **Совершайте пожертвования только чеком или банковской картой** Никогда не отдавайте деньги наличными, подарочными картами, криптовалютой или любыми средствами, которые трудно отследить. Передайте свой взнос чеком или банковской картой, чтобы гарантировать, что у вас есть запись о пожертвовании. Выписывайте чеки на имя благотворительной организации, а не на имя частного лица. Если вы решили сделать пожертвование через сайт благотворительной организации, убедитесь, что сайт безопасен и что ваш компьютер оснащен самой современной антивирусной защитой.

Если вы подозреваете, что столкнулись с мошеннической попыткой получения пожертвований, вы можете подать жалобу в Управление по защите прав потребителей штата Нью-Йорк по адресу https://dos.ny.gov/file-consumer-complaint.

Горячая линия Управления по защите прав потребителей работает с понедельника по пятницу, за исключением государственных праздников, с 8:30 о 16:30 по номеру 1-800-697-1220. Вы можете найти дополнительную информацию и советы на страницах Управления по защите прав потребителей Департамента штата Нью-Йорк (New York Department of State's Division of Consumer Protection) в Twitter (@NYSConsumer) и Facebook (www.facebook.com/nysconsumer).

На фоне возросшей международной озабоченности кибербезопасностью Департамент налогов и финансов штата Нью-Йорк также делится рядом важных советов, которые помогут налогоплательщикам защитить свою частную информацию во время налогового сезона и в течение всего года:

Опасайтесь нежелательных электронных писем и телефонных звонков с просьбой предоставить личную информацию. Никогда не сообщайте личную информацию, такую как номер социального страхования, в ответ на нежелательное электронное письмо или телефонный звонок. Если электронное письмо или звонок утверждают, что они исходят от компании, с которой вы ведете дела, позвоните ей напрямую, чтобы подтвердить законность обращения. Мошенники часто используют тактику запугивания и угрозы, связанные с налоговой задолженностью, чтобы заставить вас поделиться своей личной и финансовой информацией.

Защитите свои мобильные устройства Устанавливайте обновления программного обеспечения, которые устраняют известные уязвимости, как только они становятся доступными. Используйте встроенные в устройство средства защиты, например, код доступа, а также используйте программы, которые шифруют данные и удаленно удаляют содержимое, если устройство потеряно или украдено.

Будьте осторожны с точками доступа Wi-Fi Общественные беспроводные точки доступа не защищены, а это значит, что злоумышленники легко могут увидеть, что вы делаете на своем мобильном устройстве во время подключения. Ограничьте свои действия на общественном Wi-Fi и не входите в конфиденциальные учетные записи.

Знайте свои приложения Тщательно изучите информацию и особенности приложения, прежде чем загружать его. Изучите политику конфиденциальности каждого мобильного приложения. Имейте в виду, что приложение может запросить доступ к вашему местоположению и личной информации.

Будьте осторожны с информацией, которой вы делитесь в социальных сетях Избегайте размещения даты рождения, номера телефона, домашнего адреса, а также изображений, указывающих на вашу работу или хобби. Такая информация может быть использована для определения ответов на секретные вопросы, используемые для сброса паролей, и делает вас мишенью для

мошенников, которые пытаются получить доступ к вашим счетам и личной информации.

Используйте надежные пароли Создайте разные пароли для всех своих учетных записей. Когда речь идет о паролях, старайтесь использовать пароли, содержащие не менее 14 символов, что на сегодняшний день является отраслевым стандартом. Используйте сочетание букв (прописных и строчных), цифр и символов. Рассмотрите парольные фразы, в которых вы используете первые буквы запоминаемой фразы для создания сложного пароля, который трудно угадать. Регулярно меняйте свои пароли/парольные фразы.

Меняйте секретные вопросы. Не используйте одни и те секретные вопросы для нескольких учетных записей. Выбирайте секретные вопросы, ответы на которые нельзя угадать или найти с помощью поиска в социальных сетях или Интернете.

Используйте функцию двухэтапной проверки для доступа к учетным записям Для повышения безопасности учетных записей в Интернете по возможности требуйте пароль и дополнительный код безопасности для подтверждения вашей личности при входе в систему.

Остерегайтесь фишинга. Не нажимайте на ссылки, не скачивайте файлы и не открывайте вложения в письмах от неизвестных отправителей. Открывайте вложения только тогда, когда вы их ожидаете и знаете, что в них содержится, даже если вы знакомы с отправителем.

Важно регулярно просматривать рекомендации, необходимые для защиты конфиденциальной информации.

Сообщите о мошенничестве. Если вы стали жертвой или считаете, что можете стать жертвой кражи личных данных, связанной с налогообложением, немедленно сообщите нам об этом. Мы будем отслеживать вашу информацию, чтобы помочь сохранить ее конфиденциальность и защиту. Посетите веб-сайт Налогового департамента Сообщить о мошенничестве, аферах и краже личных данных (Report fraud, scams, and identity theft).

Налоговый департамент использует передовое шифрование, брандмауэры, системы обнаружения вторжений и другие меры безопасности для защиты наших систем и конфиденциальных данных, но налогоплательщики также должны принимать активное участие в защите себя в Интернете.

###