*Subject line:* Советы по кибербезопасности, которые помогут сохранить вашу информационную безопасность

Уважаемые жильцы NYCHA!

В связи с проведением Месяца кибербезопасности мы хотели бы представить вам некоторую информацию, которая поможет вам оставаться в кибербезопасности дома и на работе. Благодарим вас за помощь в сохранении кибербезопасности нашего мира!

## Внесите свой вклад: #BeCyberSmart (Будь кибер-умным).

Кибербезопасность - это ответственность каждого. Вы можете внести свой вклад, сообщая обо всем подозрительном, применяя более строгие меры безопасности и помогая повысить осведомленность.

## Как поднатореть в кибербезопасности

В прошлом году количество нарушений, связанных с кибератаками на американские предприятия, увеличилось на 17 процентов. Это 1,474 взлома по всей стране. Киберпреступники не просто используют технологии для кражи информации - они также полагаются на человеческие ошибки и нашу естественную склонность делиться информацией о нашей жизни.

**Будьте бдительны: достаточно одной ошибки.** Утечки данных редко являются результатом преступного взлома инфраструктуры организации. Часто они начинаются с одной уязвимости. Человека обманом заставляют сообщить свой пароль или другую информацию, и все данные, к которым у пользователя есть доступ, становятся видны. Всегда будьте бдительны насчет «фишинга» и информационно-психологических атак. Остерегайтесь необычных источников, не нажимайте на неизвестные ссылки и немедленно сообщайте о подозрительных сообщениях, связанных с NYCHA, по адресу phish@nycha.nyc.gov.

## Простые советы по обеспечению безопасности

1. Если увидели что-то - сообщите.

   Если вы заметили что-либо необычное на веб-страницах NYCHA или в прикладных программах NYCHA, сообщите об этом в Центр обслуживания клиентов NYCHA (CCC) по телефону 718-707-7771.

2. **Деловая информация - это личная информация.** Многие из нас обрабатывают конфиденциальные данные на работе. Это не обязательно должны быть номера кредитной карты или социального страхования, - это могут быть данные любого сотрудника или клиента, особенно все, что может быть привязано к конкретному человеку. Не передавайте данные компании никому за пределами вашей организации.

3. **Храните пароли разумно и надежно.** Пароли должны легко запоминаться, но трудно угадываться. Вы можете использовать фразу или серию слов, но убедитесь, что в них достаточно случайных элементов, чтобы никто не мог их угадать. Помните, особенно если

вы работаете из дома, чтобы все маршрутизаторы, сети и подключенные устройства были правильно настроены.

4. **Делайте обновления.** Периодически обновляйте свое программное обеспечение (ПО) до последней доступной версии. Убедитесь, что на всех компьютерах, которые вы используете в работе, включена защита от вирусов и вредоносных программ, и регулярно выполняйте сканирование.

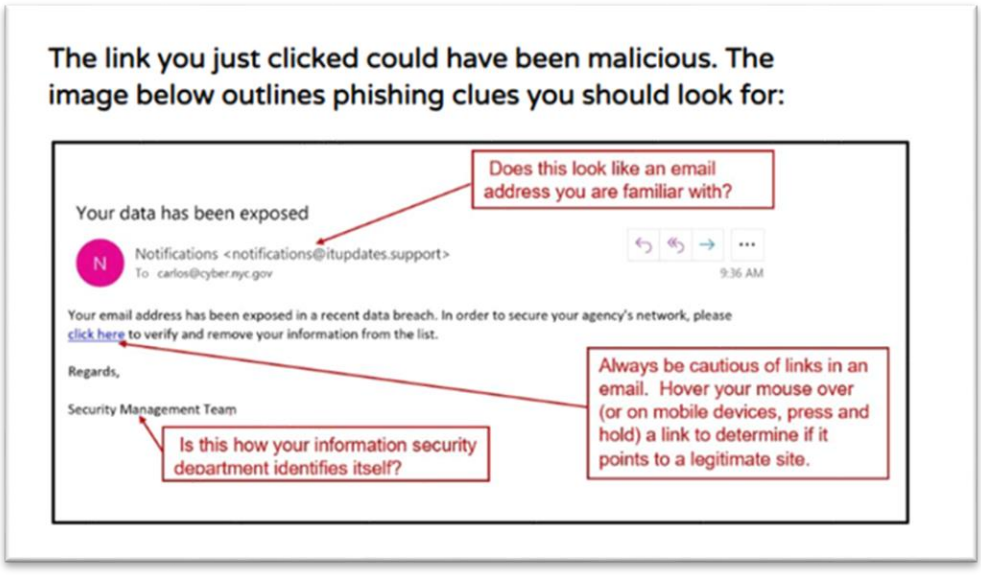
5. **Необходимость быть кибер-умным не отпадает, когда заканчивается рабочий день.** Социальные сети - это часть набора инструментов для мошенничества. Злоумышленники могут искать информацию в Google, Facebook или в любом другом месте в Интернете, чтобы получить информацию о вас. Не делитесь потенциально конфиденциальной информацией в социальных сетях или где-либо еще в Интернете и никогда не используйте социальные платформы для ведения бизнеса, связанного с работой, или обмена конфиденциальной информацией.

## Узнайте больше

Узнайте, как использовать #BeCyberSmart, просмотрев эти увлекательные видео.

## Что такое «фишинг»?

Ссылки в электронной почте, сообщениях в социальных сетях, текстах и интернет-рекламе часто являются тем, с помощью чего киберпреступники пытаются украсть вашу личную информацию. Даже если вы знаете источник, но что-то выглядит подозрительно, удалите его. Не переходите по ссылке, полученной от незнакомца. Вот несколько способов распознать попытку «фишинга»:




## Что такое «Ransomware» (программы-вымогатели)?

Программы-вымогатели - это тип вредоносного программного обеспечения, которое не позволяет вам получить доступ к вашим компьютерным файлам, системам или сетям и требует, чтобы вы

заплатили выкуп за их возвращение. Вы можете бессознательно загрузить программу-вымогатель на компьютер, открыв вложение электронной почты, нажав на объявление, перейдя по ссылке или даже посетив веб-сайт, на котором встроено вредоносное ПО. После загрузки на компьютер она блокирует доступ к нему или данным и файлам, хранящимся в нем. Обычно вы обнаруживаете, что ваш компьютер заражен, когда больше не можете получить доступ к своим данным или видите компьютерные сообщения, информирующие вас об атаке и требующие выплаты выкупа.

Лучший способ избежать программ-вымогателей - или любого другого вредоносного ПО - это быть осторожным и сознательным пользователем компьютера. Распространители вредоносных программ становятся все более искушенными, и вам нужно быть осторожным с тем, что вы загружаете и на что нажимаете.

Благодарю вас,

Greg Russ
председатель и исполнительный директор NYCHA