Памятка о безопасной работе в социальных сетях в госпабликах

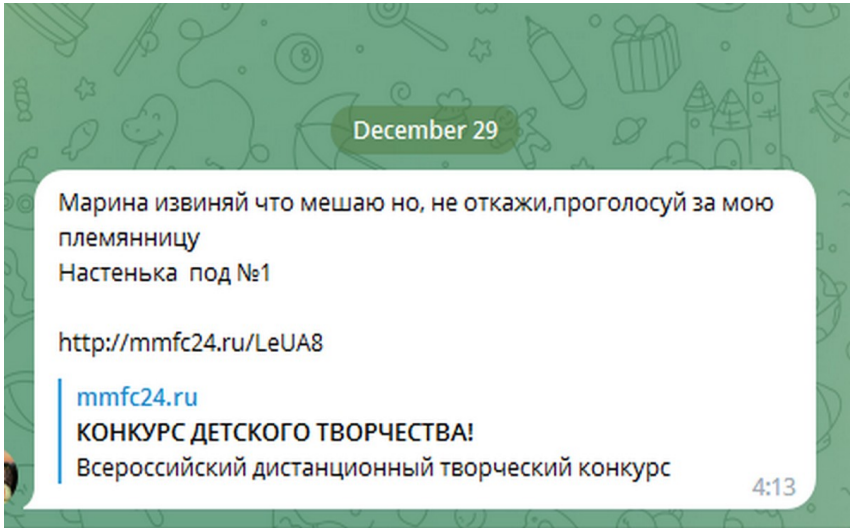
Министерство информационных технологий,
связи и цифрового развития Челябинской области

До 1 декабря 2022 года органы власти вели сообщества в социальных сетях по своему усмотрению. Теперь наличие официального аккаунта во ВКонтакте и Одноклассниках является обязательным (Федеральный закон от 14 июля 2022 г. № 270-ФЗ "О внесении изменений в Федеральный закон "Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления" и статью 10 Федерального закона "Об обеспечении доступа к информации о деятельности судов в Российской Федерации"). Перечень соцсетей был утвержден Правительством РФ в сентябре 2022 года (Распоряжение Правительства РФ от 2 сентября 2022 г. № 2523-р).

Администраторами госпабликов являются работники, имеющие личный аккаунт в социальных сетях. Для взлома официального канала органа власти достаточно похитить личный аккаунт администратора, и злоумышленник сможет скомпрометировать организацию или выложить заведомо ложную информацию. Для предотвращения таких ситуаций администраторам госпабликам необходимо придерживаться правил безопасной работы в социальных сетях, которые представлены ниже.

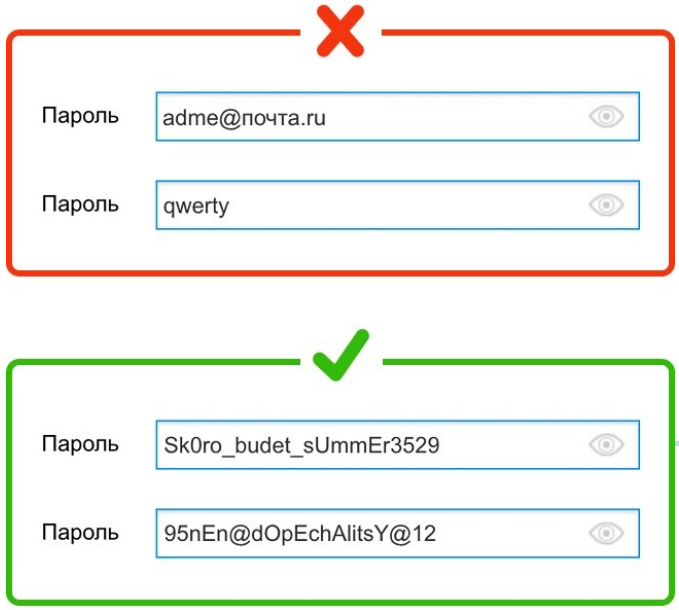
1. Самый распространенный вид компьютерной атаки, результатом которой является взлом аккаунта – фишинг. Фишинговые атаки осуществляются хакерами, которые используют подложные электронные письма или веб-сайты для кражи регистрационных данных пользователя. На почту приходит письмо, внешне очень похоже на официальное уведомление от социальной сети. Пользователь переходит по ссылке из письма на страницу идентичную сайту социальной сети, где размещена форма авторизации. Вводимый логин и пароль попадает в руки злоумышленника. Для предотвращения такого взлома, необходимо обращать внимание на адрес отправителя и адрес сайта перед авторизацией.

2. Не переходить по неизвестным ссылкам, полученным от доверенных лиц. В последнее время популярна кража данных через сообщение с просьбой проголосовать за рисунок ребенка с прикрепленной ссылкой. После нажатия на кнопку «проголосовать» открывается окно с просьбой ввести номер телефона для подтверждения голоса. После ввода номера телефона бот просит ввести высланный человеку код. На самом деле этот код является кодом подтверждения доступа к аккаунту.



3. Не используйте один и тот же пароль на различных критичных аккаунтах, которые прикреплены к госпабликам. Средний пользователь имеет порядка 26 защищенных паролем аккаунтов, но для всех этих аккаунтов он имеет всего только пять различных паролей, что порождает дополнительные риски для взлома аккаунта.

4. Не используйте очевидные и легкие пароли, которые можно угадать, собрав о вас информацию в социальных сетях. Надёжный пароль содержит 12 символов, включает буквы в разном регистре, цифры и специальные символы (~!@#$%^&*+-/.,\{}[]();:|?<>=). В нем нет последовательных комбинаций клавиш и личных данных.



5. Используйте менеджер паролей. Существует множество специальных программ, которые будут не только помнить логины и пароли, но и сгенерируют новые – ультразащищенные. Менеджер паролей это программа, которая генерирует, хранит и управляет паролями в одном безопасном аккаунте.

6. Регулярно меняйте пароли. Рекомендуется менять пароли к аккаунтам раз в три месяца.

7. Пользуйтесь двухфакторной аутентификацией. Даже если злоумышленник сможет завладеть логином и паролем от социальной сети, он все равно не сможет им воспользоваться без СМС-подтверждения.

8. Проверяйте активность профиля. Многие сервисы запоминают активность, а также присылают уведомление на смартфон или на почту, если видят, что в аккаунт входят в несвойственном пользователю регионе или стране. Данная информация позволит вовремя увидеть несанкционированное подключение к аккаунту и принять необходимые меры.