Интернет-мошенничество

С техническим прогрессом за последние пару десятилетий в нашу жизнь прочно вошли новые технологии, в том числе компьютеры, смартфоны и Интернет. Возможность совершения посредством Интернета денежных операций, онлайн-покупок и прочего при широких технических возможностях сохранения анонимности пользователя породила новый класс злоумышленников, которые промышляют интернет-мошенничеством.

Одной из разновидностей интернет-мошенничества является фишинг, главная цель которого состоит в получении конфиденциальных данных пользователей – логинов и паролей (происходит от fishing – рыбная ловля, password – пароль). Для того, чтобы в прямом и переносном смысле на попасться на уловку мошенников необходимо придерживаться ряда правил:

- следить за своими аккаунтами, при признаках подозрительной активности (взлома) которых следует ее заблокировать и обратиться к администраторам соответствующего ресурса как можно скорее;
- использовать безопасные веб-сайты, в том числе интернет-магазинов и поисковых систем, при этом нужно помнить, что часто мошенники создают сайты-двойники, чтобы пользователь по ошибке ввел туда свои данные при авторизации (логин и пароль);
- использовать сложные и разные пароли, чтобы в случае взлома злоумышленники получили доступ только к одному профилю пользователя, а не ко всем;
- в случае взлома аккаунта необходимо предупредить всех знакомых, которые указаны в друзьях у данного аккаунта, о взломе;
- рекомендуется отключить сохранение пароля в браузере;
- следует установить надежные пароль (PIN) на мобильный телефон;
- не открывать файлы и другие вложения в письмах, даже если они пришли от знакомых; при наличии подозрений, нужно уточнить, отправляли ли они эти файлы.

Помимо фишинга, интернет-мошенничество имеет много форм. Например, распространено мошенничество с использованием интернет-сервисов для размещения объявлений о товарах, недвижимости, вакансиях и прочем (например, Авито). В этом случае пользователь может лишиться своих денег, отправив предоплату злоумышленнику за товар, который не будет отправлен, или купив заведомо неисправный товар или другую вещь вместо желаемой.

В зависимости от способа мошенничества, интернет-мошенничество может быть квалифицировано по ст. 159 УК РФ (мошенничество), ст. 159.3 УК РФ (мошенничество с использованием электронных средств платежа), ст.159.6 УК РФ (мошенничество в сфере компьютерной информации). Согласно Постановлению Пленума Верховного Суда РФ от 30.11.2017 №48 мошенничество в сфере компьютерной информации, совершенное посредством неправомерного доступа к компьютерной информации или посредством создания, использования и распространения вредоносных

компьютерных программ, требует дополнительной квалификации по ст.272, 273 или 274.1 УК РФ.

Помощник прокурора
Аларского района

младший советник юстиции В.Н. Матханов