

Обман с одного клика: участились случаи хищения денег посредством фишинга

Рост случаев мошенничества с использованием средств мобильной связи в Гомельском районе удалось снизить благодаря проведенным профилактическим мероприятиям. Однако злоумышленники активизировались в другом секторе: в правоохранительные органы все чаще обращаются люди по поводу хищения денег посредством фишинга.

Реклама в интернете стала настолько привычным явлением, что большинство из нас, не задумываясь, переходит по ссылкам с любыми заманчивыми предложениями. А если скидка на товары привлекательная, мало кто удержится от соблазна тут же совершить покупку. Но здесь стоит проявить осторожность, ведь немалое количество сограждан уже стали жертвами мошенников, которые похищают деньги через фишинговые ссылки.

– Количество интернет-магазинов растет с каждым днем, сделать покупки можно даже через социальные сети. Поэтому многие покупатели не проявляют бдительности, смело вводят свои банковские и другие конфиденциальные данные в форму, предложенную для оформления покупки, производят онлайн-оплату, – отмечает первый заместитель начальника ОВД Гомельского райисполкома Юрий Рубан. *– Между тем, появилось много магазинов-однодневок. После перевода им денег вы можете не дожидаться посылки вообще, либо получить совсем не то, что ожидали.*

Такие случаи в районе фиксировались неоднократно. Доверчивые граждане оставались без денег и без покупок, после того как обслуживавший их магазин бесследно исчезал с просторов интернета. А ведь совсем несложно было предварительно навести справки о продавце, поинтересоваться отзывами и уже затем

переводить оплату.

По-прежнему часто киберпреступники работают с фишинговыми ресурсами. «Подделка» может представлять собой полную копию оригинального сайта – разница будет лишь в одном или нескольких символах в доменном имени. Граждане заходят по поддельным ссылкам в личные кабинеты на различных сервисах, а в результате предоставляют посторонним доступ к секретным сведениям.

– К любой информации в сети надо относиться с осторожностью. Мы не знаем, кто находится по другую сторону монитора – это может быть злоумышленник, – подчеркивает Юрий Рубан. – Совершая переход по ссылке, люди зачастую не осознают, насколько это значимо. Практически любой переход по ссылке запускает программу либо открывает некий ресурс, где остаются наши данные.

Сотрудники правоохранительных органов напоминают, что осторожность и бдительность, использование проверенных официальных ресурсов помогут вам защититься от посягательств злоумышленников.

Ирина Трипузова. Фото из открытых источников.