Профилактика преступлений в сфере высоких технологий

Колличество пользователей сети интернет в нашей стране постоянно растет, как и их активность. Согласно последним иследованиям. 46% белорусов делают покупки или оплачивают счета через интернет, а активные пользователи соцсетей составили 3,8 млн человек.

Высокий темп проникновения информационных технологий в нашу жизнь, наряду с неосмотрительностью некоторых пользователей, становятся предпосылки для противоправных деяний в сфере высоких технологий. За 7 месяцев 2020 года в Гродненской области зарегистрировано 729 преступлений в сфере высоких технологий, за 2019 год – 930. Из них 508 составляют хищения путем использования компьютерной техники (ст. 212 УК Республики Беларусь). Как правило, это хищение денежных средств с найденной либо похищенной банковской платежной карточки с использованием банкомата или платежного терминала. 191 из зарегистрированных в области «киберпреступлений» квалифицируются по ст. 349 УК Республики Беларусь – «Несонкционированный доступ к компьютерной информации. Например, несонкцианированный доступ к электронной почте, учетным записям на различных сайтах и в соцсетях, к информации, содержащейся на компьютере, в смортфоне и защищенной от доступа третьих лиц, Также с использованием сети Интернет нередко совершаются и другие преступления, например, мошенничество, причинение имущественного ущерба без признаков хищения, изготовление и распространение порнографических материалов или предметов порнографического характера. клевета, оскорбление, разжигание, рассовой, национальной и религиозной вражды или розни и т.п.

Чаще всего условием, играющим на руку злоумышленникам, становятся небрежное отношение владельца сайта к обеспечению сохранности конфедициальной информации о пользователях либо беспечности самих пользователей. К информации, поступающей из сети интернет, связанной с деньгами, следует относиться достаточно серьезно. Схемы мошенничества разнообразны: это и просьбы о финансовой помощи, это и выйгриши в лотерее, всевозможые, дополнительные заработки и т.д.

Чтобы не стать жертвой интернет-мошенников следует придерживаться следующих правил:

-не передавайте никому реквизиты своей карты.

-при использовании известных Вам сайтов, обращайте внимание на их внешний вид, возможно вы зашли на поддельную его копию.

-не используйте одинаковые логины и пороли на различных сайтах, слишком легкие пороли, либо те, о которых можно легко догадаться.

-остерегайтесь неожиданных или необычных электронных сообщений, даже если Вам знаком отправитель, никогда не открывайте вложения и не переходите по ссылкам в таких сообщениях.

- с осторожностью относитесь к письмам, в которых запрашиваются данные счетов, никогда не отправляйте финансовую информацию по незащищенным интернет-каналам.

- при поступлении сообщений от знакомых, содержащих побуждение к осуществлению финансовых транзакций либо передаче финансовых реквизитов, обязательно необходимо проверить данную информацию с использованием

других каналов связи (личная встреча, телефонный звонок), либо в крайнем случае идентифицируйте личность собеседника путем задачи контрольных вопросов. ответы на которые не могут быть известны третьим лицам.

Помните, если на сайте Вас просят ввести пин-код (не cvv) – 99%, что это может оказаться мошенничеством.

К сожелению, дать рекомендации о поведении в каждом возможном случае невозможно, но в общем случае, можно предложить пользователям в любой ситуации не терять бдительность и критическое отношение к окражающим нас явлениям и событиям.

Начальник ООПП МОБ РОВД Д. Н. Ксенжук

Увлекаешься информатикой?
Используешь знания незаконно?
Нравиться взламывать чужие сайты?

Отлично
Преступно
Наказуемо

ВНИМАНИЕ!!! Ответственность с 14 лет

Статья 212 Уголовного кодекса: хищение имущества путем использования компьютерной техники, либо путем введения в компьютерную систему ложной информации *(фишинг)* наказывается вплоть до лишения свободы на срок до 3 лет.
Те же действия, совершенные повторно, либо в группе по предварительному сговору – на срок до 5 лет.

Всё тайное всегда когда-то становится явным
Статья 349 Уголовного кодекса: несанкционированный доступ к информации, хранящейся в компьютерной системе, сети или на машинных носителях, сопровождающийся нарушением системы защиты *(несанкционированный доступ к компьютерной информации)*, повлекший по неосторожности изменение, уничтожение, блокирование информации или вывод из строя компьютерного оборудования либо причинение иного существенного вреда наказывается *штрафом* или *арестом.*
Те же действия, совершенные из корыстной или иной личной заинтересованности, – на срок до 2 лет, а повлекшие по неосторожности крушение, аварию, катастрофу, несчастные случаи с людьми, отрицательные изменения в окружающей среде или иные тяжкие последствия, - на срок до 7 лет.
***ФИШИНГ* – не рыбалка! *Преступление* – не развлечение!**

МВД РЕСПУБЛИКИ БЕЛАРУСЬ