**Фишинг и не только. Какие преступления в виртуальном пространстве совершают подростки**

Все чаще подростки совершают преступления и правонарушения с использованием виртуального пространства. Подростки в сети - интернет испытывают на себе унижение, оскорбление, насмешки - так называемый кибербуллинг. Они сталкиваются с информацией, содержащей насилие, пропаганду самоубийства и психоактивных веществ, нетрадиционные сексуальные отношения, несовершеннолетние становятся жертвами киберпреступлений.

**К основным видам киберпреступлений в сети - интернет относятся:**

**Кетфишинг -** второе место в статистике киберпреступлений, это когда человек выдает себя в Интернете за другую личность, используя чужие фото и имя.

**Сексторция -** третий по популярности вид киберпреступлений, это угроза выложить в Интернет интимные фото жертвы как принуждение к чему-то - например, заплатить выкуп.

**DoS-атака -** хакерская атака на вычислительную систему с целью вывести ее из строя. Удобный способ оказать давление, не оставляя за собой улик.

Если атака выполняется с большего числа компьютеров, она называется DDoS-атака - сокращение от Distributed Denial of Service, то есть «отказ в обслуживании». Причем владельцы компьютеров могут даже не знать, что участвуют в хакерской атаке. Такие компьютеры называются компьютерами-зомби: злоумышленник взламывает слабый узел, устанавливает на него троянскую программу - и с этого момента жертва участвует в коллективной атаке на целевой компьютер.

**Доксинг -** публикация в сети - интернет конфиденциальной информации о человеке без его согласия. Доксинг не преследуется законом, но считается нарушением сетевого этикета и запрещен внутри интернет-сообществ. Что, впрочем, не мешает пользователям им заниматься.

**Интернет-травля -** или кибербуллинг - травля в Интернете одного человека группой людей. Чаще всего одноклассника подростками.

Одним из самых опасных и эффективных способов кибератаки в сети- интернет является фишинг.

**Фишинг** (от англ. fishing - рыбная ловля) - противоправное действие, совершаемое с целью заставить то или иное лицо поделиться своей конфиденциальной информацией, т.е. это совокупность методов, позволяющих обмануть пользователя и заставить его раскрыть свой пароль, номер кредитной карты либо другую конфиденциальную информацию. Чаще всего злоумышленники выдают себя за представителей известных организаций в электронных письмах или телефонных звонках.

Одной из наиболее распространенной тактикой фишинга является метод, который позволяет «поймать на крючок» свою жертву. Как это происходит?

Жертва получает электронное письмо или текстовое сообщение, отправитель которого [выдает себя](https://www.techopedia.com/definition/5398/spoofing) за определенное лицо или организацию, которым жертва доверяет, например за коллегу по работе, сотрудника банка или за представителя государственного учреждения. Когда ничего не подозревающий получатель открывает это электронное письмо или сообщение, то он обнаруживает пугающий текст, специально составленный таким образом, чтобы подавить здравый смысл и внушить страх. Текст требует от жертвы перейти на веб-сайт и немедленно выполнить определенные действия, чтобы избежать опасности или каких-либо серьезных последствий.

Если пользователь «клюет на наживку» и переходит по ссылке, то он попадает на веб-сайт, имитирующий тот или иной законный интернет - ресурс. На этом веб - сайте пользователя просят «войти в систему», используя имя своей учетной записи и пароль. Если он оказывается достаточно доверчивым и соглашается, то введенные данные попадают напрямую к злоумышленникам, которые затем используют их для кражи конфиденциальной информации или денежных средств с банковских счетов.

К основным типам (категориям) фишинговых атак относятся:

*адресный фишинг* - это когда злоумышленники атакуют конкретное лицо или организацию, часто применяя специально подобранный контент, который окажет на жертву наибольшее воздействие;

*клоновый фишинг* - данныйтип атаки предполагает, что злоумышленники копируют (клонируют) ранее доставленное законное сообщение, которое содержит ссылку или вложение. Затем мошенник меняет ссылки или прилагаемые файлы на вредоносные объекты, выдаваемые за настоящие. Ничего не подозревающие пользователи нажимают на ссылку или открывают вложение, чего часто бывает достаточно для хакеров, чтобы перехватить контроль над компьютером. После этого злоумышленники могут маскироваться под надежных отправителей и рассылать от имени жертвы аналогичные электронные письма другим пользователям в пределах этой же организации;

*телефонный фишинг* - это когда фишинговые атаки происходят с помощью обычного телефона - в этом случае они иногда обозначаются как голосовой фишинг или *«*[*вишинг*](https://blog.malwarebytes.com/glossary/vishing/)*»,* т.е. мошенник звонит своей жертве и представляется сотрудником местного банка, полиции или налогового управления. Затем он запугивает жертву, сообщая о какой-либо проблеме и настаивая на том, что ее необходимо решить немедленно, а для этого нужно сообщить ему данные банковского счета или выплатить штраф. Обычно мошенники требуют перечислить деньги безналичным способом или с помощью предоплаченной карты, чтобы их нельзя было отследить;

[*SMS-фишинг*](https://blog.malwarebytes.com/cybercrime/2015/08/new-smishing-campaign-targets-t-mobile-subscribers/)*(или «смишинг»)* - это брат - близнец вишинга, осуществляющий те же мошеннические действия, но только с помощью SMS-сообщений (иногда добавляя к ним вредоносные ссылки).

**Как распознать фишинговую атаку?**

**1.**Обращать внимание на все, что кажется странным и необычным. Фишинговые атаки часто используют страх, чтобы подавить Вашу способность хладнокровно мыслить.

**2.**В электронном письме получатель находит предложение, которое выглядит слишком выгодным, чтобы быть правдой. В нем может сообщаться, что Вы выиграли в лотерею, получили дорогой приз или какой-либо уникальный предмет.

**3.** Текст сообщения внушает страх. Будьте бдительны, если текст электронного письма носит угрожающий или тревожный характер и стремится создать атмосферу неотложной ситуации, призывая Вас срочно выполнить те или иные действия, например перейти по ссылке, прежде чем Ваша учетная запись будет заблокирована. Помните, что ответственные организации никогда не просят клиентов передать персональные данные через Интернет.

**4.**Сообщение содержит неожиданные или необычные вложения. Такие вложения могут содержать вредоносное ПО, программы-вымогатели или другие интернет-угрозы.

**5.**Сообщение содержит ссылки, которые выглядят странно.

**Как защититься от фишинга?**

**1.**Не открывайте электронные письма от незнакомых отправителей.

**2.**Нажимайте на ссылку внутри электронного письма только в том случае, если Вы точно знаете, куда она ведет.

**3.**Получив письмо от сомнительного отправителя, перейдите по прилагаемой ссылке вручную - введите адрес законного веб-сайта в адресную строку браузера с помощью клавиатуры, так Вы обеспечите для себя еще один уровень безопасности.

**4.**Проверяйте цифровые сертификаты веб-сайтов.

**5**.Если Вы подозреваете, что полученное электронное письмо было отправлено мошенником, введите имя отправителя или отрывок текста письма в поисковую систему - и Вы увидите, связаны ли с этим письмом какие-либо фишинговые атаки.

**6**.Необходимо использовать программу, способную противостоять вредоносному программному обеспечению. Большинство программных средств кибербезопасности способны обнаруживать маскирующиеся опасные ссылки и вложения, так что Ваша информация не попадет в руки злоумышленников, даже если Вы вовремя не почувствуете неладное.