Модуль №4
ПОТРЕБЛЕНИЕ

Интернет оказал влияние на все сферы нашей жизни, в том числе и на сферу услуг. Благодаря новым технологиям мы можем делать покупки онлайн в любых магазинах мира. А Интернет в данном случае выступает в качестве удобного средства потребления: выбора, оценки, заказа и оплаты товаров.

Наряду с очевидными преимуществами покупок онлайн — экономия времени, более низкие цены, огромный ассортимент — существуют и определённые потребительские риски.

Многие из них нам знакомы из реальной жизни: недостоверная реклама, поддельный или некачественный товар, махинации с платежами.

В виртуальном мире киберпреступники пытаются завладеть персональной информацией пользователей для хищения денежных средств. Поэтому твои знания о работе в Интернете должны включать в себя и навыки безопасного потребления. Научись распознавать действия мошенников и противостоять им.

СОДЕРЖАНИЕ

1. Фишинг
2. Психологические приёмы мошенников
3. Реклама
4. Правила безопасных покупок онлайн
5. Игры

Фишинг

Фишинг — это одна из наиболее распространённых форм мошенничества. Задача фишинга — выудить персональные данные у пользователя, чтобы потом использовать их в преступных целях.

В арсенале у злоумышленников — методы, основанные на знании человеческих слабостей и действий, которые мы совершаем на автомате, не задумываясь.

Тебе сообщают, что ты стал миллионным посетителем сайта, предлагают планшетный компьютер в обмен на заполнение анкеты или обещают рассказать о быстром и лёгком заработке? Будь осторожен: это типичная уловка.

Не спеши заполнять анкету! Даже если требуется сообщить безобидные, на первый взгляд, сведения: фамилию, имя, адрес и номер телефона. Зачастую достаточно ввода данных без нажатия кнопки «Отправить», чтобы мошенники завладели информацией.

Для того чтобы заполучить личную информацию пользователей, кибермошенники создают поддельные фишинговые сайты, которые по своему оформлению могут ничем не отличаться от сайтов реальных организаций, например банков.

Получив от знакомого странное сообщение с просьбой перевести денег либо ссылку на подозрительную заметку или видео, будь осторожен: возможно, аккаунт друга взломан и тебе пишет мошенник, а ссылка ведёт на фишинговый сайт. Любая информация, оставленная на таком сайте, попадает в руки мошенников.

Что делать, если ты стал жертвой интернет-мошенничества:

1. Смени все пароли и свяжись с администрацией сайта, на котором произошла кража данных.
2. Не теряй времени, дожидаясь ответа от службы поддержки, — обратись за помощью к взрослым.
3. Не пытайся бороться с мошенниками самостоятельно. Это опытные люди, которые хорошо владеют ситуацией.

Как избежать мошенничества и не стать жертвой фишинга
http://www.google.com/goodtoknow/online-safety/scams/

Приемы мошенников

Кибермошенники используют хитрые приёмы, которые позволяют воздействовать даже на тех, кого не назовёшь доверчивым или наивным. Однако зная уловки мошенников и критично оценивая происходящее, ты сможешь противостоять манипулированию.

Изучи, какие приёмы используют мошенники:

1. **В сообщении содержится просьба или угроза не разглашать его содержание третьим лицам.**

2. **Прямо или косвенно запрашивается передача личных данных и финансовой или секретной информации** (паролей, PIN-кодов, номера банковской карты и пр.).

3. **Копируется дизайн и стилистика известных брендов в расчёте на доверие к крупным компаниям.**

4. **Чтобы заглушить голос рассудка, идёт апелляция к сильным эмоциям:**

— угрозы здоровью, безопасности счетов и аккаунтов;
— обещания большой денежной выгоды;
— неправдоподобно выгодные условия покупки или акции;
— запросы о пожертвованиях от лица благотворительных организаций.

5. **Используется персональное обращение.**

6. **В приказной форме предлагается совершить какие-либо из следующих действий:**

— ответить в течение нескольких дней;
— не упустить заманчивое предложение, которое действует всего неделю;
— срочно перейти по ссылке, иначе банковский счёт или аккаунт в социальной сети будут заблокированы навсегда.

Как реагировать на фишинговые сообщения?

1. Обрати внимание на **адрес отправителя**: как правило, фишинговые сообщения приходят с незнакомых или подозрительных адресов.

2. **Проверь информацию в письме**: прозвони, зайди на официальный сайт, сделай запрос в поисковике.

3. Если сообщение содержит **угрозу для жизни и здоровья близких людей** , свяжись с ними, чтобы убедиться в их безопасности. Подумай, где и с кем они могут сейчас находиться.

4. Помни: **никакой банк или официальное лицо НИКОГДА не запросит** твоих личных данных, пересылки паролей или секретных кодов!

5. Подумай, **откуда незнакомый человек мог получить** твою персональную информацию, и постарайся максимально ограничить доступ к ней.

6. Оцени грамотность письма, логику изложения: как правило, в письме много ошибок, неточностей и противоречий.

— Если убедился, что сообщение фишинговое, — удали его!

Также помни о том, что в большинстве случаев правильнее не открывать электронные сообщения от незнакомых адресатов и сразу удалять письма, в теме которых содержатся предложения неправдоподобных акций или информация о том, что ты выиграл неожиданный приз. В них могут содержаться вирусы, способные повредить компьютер.

Остерегайся мошенничества в Интернете
http://youtu.be/AMCsvZXCd9w

Реклама

Интернет не может существовать без рекламы. Работа таких сервисов, как бесплатные почтовые ящики, социальные сети, поисковики, во многом обеспечивается за счёт средств, полученных от рекламы.

Иногда реклама в Интернете может содержать ложную информацию или вести на опасные сайты. Поэтому относись к рекламе осторожно. Не кликай на завлекающие картинки (на то и расчёт!), а сведения рекламных сообщений тщательно перепроверяй.

Со своей стороны, компания Google разработала чёткие правила в отношении рекламы. Не разрешается рекламировать сайты с вредоносным ПО, поддельными товарами и непрозрачной системой оплаты.

И если Google находит мошенническое объявление, то он не просто его блокирует, а прекращает сотрудничать с рекламодателем, который его разместил.

Правила безопасных покупок онлайн

Интернет выводит процесс совершения покупок на новый уровень. Например, можно приобрести долгожданную книжку в день выхода, успеть купить классные джинсы на распродаже или устроить сюрприз другу — заказать на день рожденья подарок с доставкой на дом.

Но пользуясь услугами интернет-магазинов, как и в реальной жизни, нужно соблюдать определённые правила:

1. Совершай покупки в крупных **интернет-магазинах, хорошо зарекомендовавших себя на рынке**.

2. Внимательно ч**итай условия предоставления услуг**, а также все документы, получаемые при оформлении заказа, например, бланк заказа, товарные накладные, счета и т. д.

3. Проверь **реквизиты продавца**, особенно если магазин не вызывает доверия.

4. Запроси **подтверждения законности торговой деятельности**, убедись, что представленный знак качества или сертификат являются настоящими.

5. Не доверяй магазину только **потому, что у сайта красивый дизайн**.

6. Читай **отзывы покупателей о магазине**, размещённые на сторонних сайтах. Хотя исключить вероятность того, что эти отзывы заказные, всё равно нельзя.

7. Узнай через поисковик или по дате регистрации домена, **как долго существует магазин.**

8. Сравнивай цены в разных интернет-магазинах с помощью сервиса «Яндекс.Маркет» или «Покупки Google». **Слишком низкая цена говорит о подделке** или недобропорядочных намерениях продавца.

9. Уточни по телефону **конечную стоимость товара и его доставки, условия выполнения заказа, возможность получения кассового чека**. Оцени уровень культуры общения продавца.

10. Помни: НИКОГДА и ни при каких условиях добросовестный продавец **не будет запрашивать PIN-код банковской карты или пароль от аккаунта**. Если это произошло, сразу же прекрати все действия на сайте и свяжись с представителями банка, выпустившего карту, для того чтобы её заблокировать.

Игры

Онлайн-игры, как любое развлечение, приносят радость и поднимают настроение. Однако иногда игра из увлечения может превратиться в зависимость или инструмент манипулирования.

Чтобы этого не произошло, соблюдай простые правила:

1. Внимательно изучи **пользовательское соглашение**: какие обязательства ты на себя принимаешь, что ждёт тебя в самой игре и каких вложений она потребует от тебя в будущем.

2. Узнай, что **думают об игре другие пользователи**, какие проблемы у них возникают и как служба поддержки помогает их разрешить.

3. Опасный сигнал, если во время игры требуется **рассылка приглашений и других сообщений** твоим друзьям.

4. Если чувствуешь, **что тебе трудно прекратить игру и ты теряешь счёт времени**, попробуй ограничить своё пребывание в игре с помощью будильника.

5. Если сценарий игры **предполагает трату денег для перехода на другой уровень** или регулярного посещения странички игры, самым разумным будет прекратить эту игру.

6. Если игра вызывает злость, раздражение, усталость или тебе трудно прекратить её, используй самый радикальный и эффективный метод: **удали игровой аккаунт и программу.**

Выводы

Интернет-потребление может быть сопряжено с определёнными рисками. Ответственное отношение к собственной безопасности и понимание основных приёмов интернет-мошенников помогут уберечься от кражи личных данных.

Соблюдение секретности персональных данных, отказ от любых форм взаимодействия с незнакомыми пользователями, критичное отношение к получаемым интернет-сообщениям, перепроверка информации — всё это должно стать твоей привычкой.

Перед совершением интернет-покупок убедись в надёжности продавца. Изучи информацию о нём в Интернете, посмотри отзывы, пообщайся по телефону. Всё ещё сомневаешься — спроси совета у взрослых.

Помни, что так любимые тобой онлайн-игры могут содержать скрытые риски и угрозы. Не играй по правилам манипуляторов! Если теряешь контроль над ситуацией, лучше перестать играть в эту игру вообще или удалить её. И счёт в итоге будет в твою пользу!