Государственное бюджетное учреждение культуры Архангельской области
«Архангельская областная научная ордена “Знак Почета”
библиотека имени Н. А. Добролюбова»

Электронный читальный зал

Интернет-угрозы для пользователей старшего возраста и правила безопасности

Методические рекомендации

Часть 1. Общие правила безопасности пользования Интернетом

Архангельск
2020

Интернет-угрозы для пользователей старшего возраста и правила безопасности : методические рекомендации : в 4 частях. Часть 1. Общие правила безопасности пользования / Архангельская областная научная библиотека им. Н. А. Добролюбова ; [сост. И. А. Макаренко, Н. М. Горланова]. – Архангельск, 2020. – 12 с.

Настоящее пособие продолжает череду методических материалов, подготовленных Архангельской областной научной библиотекой им. Н. А. Добролюбова в помощь сотрудникам муниципальных библиотек по формированию у читателей цифровой культуры. Цифровая культура — неотъемлемая часть повседневной культуры человека, живущего в современном обществе и активно пользующегося его возможностями и благами. Она подразумевает умение грамотно применять информационные технологии в работе, учебе и быту, а также осознанный, разумный подход в обращении к Интернету и его сервисам.

Некоторые специалисты разделяют понятия «цифровая грамотность» и «цифровая компетентность». Последнее они трактуют шире и относят к нему не только знания и навыки, но и ответственность человека, его умение критически оценивать информацию, получаемую через Интернет. Люди, обладающие такими умениями и знаниями, способны максимально безопасно пользоваться возможностями, которые дает им жизнь в цифровой среде.

Именно о безопасном пользовании Интернетом пойдет речь в нашем пособии. Мы расскажем о рисках, которые подстерегают неискушенных пользователей, и способах защиты от них. Библиотекари найдут здесь материал, который мы рекомендуем использовать в ходе занятий с читателями по формированию знаний и навыков в обращении с компьютером. Помимо теоретической части мы предлагаем интерактивные формы — обсуждения и тесты. Они помогут слушателям закрепить полученную информацию.

Целевая аудитория посетителей библиотек, на которую рассчитан предлагаемый материал, — люди старшего возраста. Ввиду малого опыта пользования компьютером и Интернетом, а также в силу особенностей воспитания и мировоззрения они так же уязвимы в интернет-среде, как дети и подростки. Только опасности, которые подстерегают тех и других, разнятся. Если самостоятельность детей в Интернете рекомендуется ограничивать, а также обучать их правилам психологической самозащиты и обращаться за помощью к родителям, то взрослые люди должны уметь сами регулировать свою безопасность, распознавать финансовые угрозы, оценивать достоверность и репутацию ресурсов, чтобы избежать мошенничества и агрессии по отношению к себе.

Наше пособие будет состоять из нескольких частей: «Общие правила безопасности работы в Интернете», «Безопасность коммуникации в Интернете», «Потребительская безопасность в Интернете», «Достоверность информации в Интернете».

Интернет повлиял на очень многие аспекты жизни пользователей старшего возраста. Люди отвыкли искать ответы на вопросы в бумажных справочниках или справляться по телефону, делать фотоальбомы, писать и посылать по почте поздравительные открытки и письма, предпочитая отправлять короткие текстовые сообщения вместо долгого телефонного разговора, фотографировать нужную информацию вместо записывания ее, а также платить по электронным квитанциям, получать онлайн-талоны на прием к врачам и проч. Изменилось потребительское поведение. Пожилые пользователи делают покупки в Интернете, совершают там различные финансовые операции. Они быстро находят информацию, потребность в которой появляется «здесь и сейчас».

Преимущества Интернета для старшего возраста очевидны. Темп их жизни стал более динамичным, расширились социальные связи, изменилась форма мышления, уменьшился межпоколенческий разрыв. Но вместе с новыми возможностями Интернет принес и новую ответственность, и необходимость распознавать опасности, угрозы.

Какие виды угроз существуют?

Исследователи выделяют следующие интернет-риски.

Контентные риски. Они возникают в процессе просмотра находящихся в Сети материалов (текстов, картинок, аудио- и видеофайлов, ссылок на различные ресурсы), содержащих противозаконную, неэтичную и вредоносную информацию.

Коммуникационные риски. Возникают в процессе межличностного взаимодействия пользователей в Сети. С коммуникационными рисками можно столкнуться при общении в чатах, онлайн-мессенджерах, социальных сетях, на сайтах знакомств, форумах, в блогах.

Потребительские риски. Возникают в процессе приобретения товаров и услуг через Интернет. Они включают риск получения товара низкого качества, контрафактной и фальсифицированной продукции, риск потери денежных средств без доставки товара или услуги, хищения финансовой информации с целью мошенничества.

Технические риски. Здесь возможны повреждения программного обеспечения компьютера, нарушение конфиденциальности информации, взлом аккаунтов, хищение паролей и персональных данных посредством вредоносных программ.

Для начала вспомним основные правила безопасного пользования Интернетом, которые помогут уберечь компьютер или другое устройство от поломки и утечки персональной информации.

Как выбрать антивирусную программу?

Самая распространённая интернет-угроза — это атака вирусов. Из-за неё можно потерять информацию, хранящуюся на компьютере, а также повредить свое оборудование и программное обеспечение. Как вирусы попадают в компьютер? В домашних условиях есть два пути: через Интернет и через съемный носитель. Например, в компьютер достаточно вставить флешку, подключить жесткий диск, свой или чужой, но побывавший в другом, зараженном компьютере. Самый распространённый путь заражения компьютерным вирусом — заражение через Интернет. По каким каналам оно происходит?

Вредоносные сайты. Пользователь открывает страницу, которую нашел в поисковике или получил на нее ссылку в сообщении, кликает по привлекшему его баннеру и попадает на «опасный» сайт. Там присутствует код, который запускает определенное действие, например автоматическое скачивание вредоносного файла. Пользователь может случайно щелкнуть по картинке или на значок незнакомой программы и своими руками запустить вирус.

Электронная почта. Вирус может находиться в самом письме в форме ссылки или во вложениях к нему. Такое письмо придет от неизвестного отправителя, вы откроете его, перейдете по предложенной ссылке или просто откроете вложение, в котором спрятался вирус. Те, кто рассылают подобные письма, хорошо разбираются в психологии людей и поэтому выбирают такие темы писем, которым очень сложно противостоять, чтобы не открыть их (например: «с вашего счёта списано 5673 руб.», или «ваш счёт пополнен», или «вы выиграли…»). Опасное письмо может прийти и от знакомого человека, например от друга, компьютер которого заражен таким вирусом, и вирус автоматически рассылает себя всем, кто есть в адресной книге.

Вредоносное программное обеспечение. Вы устанавливаете взятую из Интернета необходимую вам программу, например для просмотра видео или для скачивания музыки из соцсети «ВКонтакте», а она заражена вирусом. Это касается бесплатных программ на неофициальных сайтах. Здесь, как и в случае с любым непроверенным файлом,

скачанным с ненадежного сайта, вы думаете, что скачиваете одно, а под видом нужного файла запускается вредоносное программное обеспечение.

Социальные сети. Отсюда вирус может попасть двумя способами: через личные сообщения и через установку приложений. Неизвестный вам человек (или известный, но «взломанный») пишет вам личное сообщение, в котором есть ссылка или вложение. Вы запускаете его, и всё происходит по такому же сценарию, как с электронными письмами и вредоносными сайтами. Другой вариант: вы устанавливаете какое-нибудь полулегальное приложение, чтобы «посмотреть, кто заходил на твою страничку» или «скачать музыку бесплатно», и тем самым закачиваете себе вирус.

Чтобы избежать проникновения вирусов на электронное устройство, следите за регулярным обновлением операционной системы на нем и пользуйтесь антивирусными программами. Они устранят многие угрозы, подскажут, можно ли посещать неизвестный вам сайт. Выбор антивирусной программы часто становится непростой задачей, потому что таких программ существует множество — платных и бесплатных.

Чтобы получить максимальную выгоду от использования антивируса, рекомендуется выбирать проверенные программы — те, о которых часто говорят или пишут, и не использовать несколько антивирусных программ на одном компьютере. Платную или бесплатную программу выбрать? Безусловно, качество защиты вашего компьютера напрямую зависит от стоимости программы, однако бесплатные версии неплохо справляются с базовыми задачами. Часто бесплатной версии вполне достаточно, чтобы защитить домашний компьютер от основных угроз.

Так на чем остановиться? Как найти среди множества предложений то, которое подходит вам? Поочередно, устанавливая и удаляя несколько антивирусов, можно протестировать работу нескольких и решить, что именно выбрать. Многие антивирусные лаборатории предлагают бесплатный тридцатидневный тестовый режим для своих продуктов. Выбирая антивирус, учитывайте мощность вашего компьютера. Если компьютер слабоват — лучше пробовать программу с небольшим потреблением оперативной памяти, чтобы не нагружать операционную систему (например, AVG AntiVirus). Если компьютер постоянно подключен к Интернету — необходимо выбирать антивирус, содержащий в себе сетевой экран, который защищает от всплывающих окон и попадания на вредоносные сайты. В выборе антивирусной программы можно руководствоваться рейтингами, которые проводятся независимыми лабораториями. Такие рейтинги легко найти в Интернете, например: 10 лучших антивирусов в 2020[1] или Рейтинг лучших антивирусов 2020 для дома и офиса[2]. Здесь можно узнать о реальной эффективности того или иного антивирусного продукта. Выбирая между платным и бесплатным вариантами антивирусной программы, следует отдавать себе отчет, насколько важная информация хранится на компьютере. Если вы платите за антивирус деньги — при необходимости вам будет оказана оперативная поддержка, при использовании бесплатной программы — нет. Если вы все-таки выбираете бесплатный антивирус, то не пользуйтесь малоизвестными программами, они не дадут достаточной защиты вашей системе.

Предлагаем перечень лучших антивирусных программ:

---

[1] Джексон С. 10 лучших антивирусов в 2020 // SafetyDetectives : сайт. 2020. URL: https://ru.safetydetectives.com/ – Дата публикации: 30.09.2020.

[2] Рейтинг лучших антивирусов 2020 для дома и офиса // WindowsGuide.ru : сайт. URL: https://windowsguide.ru/software/top-antivirusov-2019/ (дата обращения: 14.10.2020).

Бесплатные антивирусы	*Платные антивирусы*
Avast! Free Antivirus	Антивирус Касперского
AVG Anti-Virus Free	ESET NOD32
Avira Antivirus	Dr.Web
Comodo Antivirus	Panda Antivirus Pro
Zillya	

Важно помнить, что даже самый дорогой и популярный антивирусный продукт необходимо своевременно обновлять, потому что именно вместе с обновлениями программа получает информацию о новых вирусах и способна им противостоять.

Каким должен быть пароль?

Однако в случае вашей же собственной невнимательности ни один антивирус не сможет защитить вас. В настоящее время в Сети гораздо чаще приходится сталкиваться не с вирусными атаками, а с мошенниками, пытающимися выманить ваши деньги, используя всевозможные обманные схемы.

Общаясь в социальных сетях, пользуясь электронной почтой, интернет-магазинами, онлайн-банками, мы сообщаем в своих личных профилях множество персональных данных. С одной стороны, это существенно упрощает жизнь — данные всегда под рукой. Но в случае, если паролем от вашей страницы завладеет злоумышленник, ваши финансы и репутация могут сильно пострадать. Вот почему так важно защищать свои личные страницы надежными паролями.

Существует несколько основных правил создания паролей:

1. Используйте хотя бы одну заглавную букву.
2. Используйте хотя бы одну цифру.
3. Не указывайте в пароле ваше имя / фамилию /дату рождения / номер телефона — иначе говоря, основные данные, которые можно найти в соцсетях.
4. Используйте более 8–10 символов. Чем длиннее ваш пароль, тем лучшей защитой он является.
5. Не используйте один и тот же пароль для всех или даже нескольких сервисов, на каждый сервис — отдельный пароль.
6. Не используйте буквы и цифры, идущие по порядку. Например: 12345, qwerty и т. д., а также любые варианты слова «пароль».

Любой, даже самый надежный пароль необходимо суметь сохранить в тайне. К сожалению, идеального способа, как это сделать, не существует. Тем не менее, вот несколько вариантов с их плюсами и минусами:

1. Запомнить. В этом случае он будет известен только вам. Но главный недостаток здесь в том, что пароль можно забыть. К тому же почти невозможно запомнить несколько разных паролей.
2. Записать. Такой способ предпочитает старшее поколение. Хранить записанный пароль или пароли нужно в каком-то надежном месте, например с документами. Неоспоримый плюс хранения паролей на бумаге — невозможность постороннего онлайн-доступа. Минус — вероятность потери листка с записями.
3. Текстовый файл на компьютере. Из файла удобно копировать пароли парой кликов. Но при несанкционированном доступе к вашему компьютеру данные могут быть украдены. Второй важный минус в том, что пароли доступны только на том компьютере, на котором хранится документ.
4. Текстовый файл на внешнем накопителе — флешке или диске. Их удобно носить с собой — файл с паролями всегда под рукой. Но, как и с бумажным вариантом, флешку можно потерять, и вы утратите учетные данные, в худшем случае — они станут доступны третьим лицам.

5. Файл в облаке. Удобство хранения документов в облаках — в их доступности с любых устройств в любом месте, где есть Интернет. Файлы с паролями можно размещать в виртуальных хранилищах, например, в Яндекс- и Google-дисках, в Microsoft One Drive или в онлайн-блокнотах вроде Evernote. Основной опасностью данного метода является возможность случайного открытого доступа посторонних лиц к папке с файлом.
6. Автозапоминание в браузере. Функция сохранения пароля существует во многих браузерах. Разумеется, это упрощает процесс авторизации, однако пароль может быть удален при обновлении программы или чистке кэша. К тому же, если веб-страница помнит ваш пароль, ею могут воспользоваться посторонние в ваше отсутствие возле компьютера. Если вы захотите воспользоваться таким способом хранения пароля, то мы рекомендуем делать это на вашем личном домашнем компьютере, за которым больше никто не работает.

Ограничивать ли доступ к камере, микрофону и геолокации?

Существуют и другие, менее распространенные технические риски. Это, например, использование злоумышленниками ваших веб-камер и камер в телефоне, а также микрофонов. Рекомендации заклеивать видеокамеру ноутбука часто можно услышать даже от ведущих специалистов в сфере электронных технологий, а также увидеть фотографии, на которых эти люди сами заклеили камеры на своих ноутбуках.

С одной стороны, техническая возможность незаметно следить за кем-то посредством веб-камеры или микрофона существует. Существуют вирусы, ведущие запись с камеры и передающие данные без ведома владельца, вирусы, запоминающие все нажатия клавиатуры пользователем, вирусы, записывающие происходящее на экране.

С другой стороны, маловероятно, что взломщик высокого уровня заинтересуется именно вашим компьютером, да и защитные программы постоянно принимают меры против взлома и расширяют свои возможности. Так что регулярное обновление антивирусной программы и осознанное использование Интернета (не посещать подозрительные сайты, не открывать ссылки и вложения) обезопасят от этой угрозы.

Иногда разрешение на доступ к камерам и микрофонам просят приложения, которые, казалось бы, не должны использовать их. Такие запросы лучше отклонять. То же самое касается и запросов геолокации от мобильных приложений и сайтов. Например, если приложение с интерактивной картой города просит данные о вашем местоположении, то этот запрос не очень подозрителен и его можно подтвердить. Такой же запрос от интернет-магазина тоже оправдан (кстати, эти данные можно ввести и вручную). А, например, подобный запрос от фоторедактора или игры уже будет выглядеть подозрительно.

Мобильные приложения также могут отправить запрос на использование камеры или микрофона. Если это, допустим, хорошо известное приложение для видеозвонков (например, Skype), скачанное с его официального сайта, то разрешение можно дать. В противном случае этого делать не стоит.

Приложение, запросившее подозрительные разрешения, стоит удалить.

Вопросы для обсуждения

Эти вопросы мы предлагаем задавать слушателям обучающего семинара перед изложением каждого нового фрагмента теоретического материала.

— Что такое Интернет? Как он влияет на образ жизни людей (вас и ваших знакомых)?
— Какие возможности Интернета кажутся вам наиболее полезными?
— О каких рисках и опасностях Интернета вы слышали?

— Как вы думаете, какой пароль будет труднее всего взломать?
— Какой способ хранения пароля кажется вам самым удобным?
— Есть ли техническая возможность шпионить за вами через ваш компьютер?
— Знаете ли вы еще какие-то способы защиты своего компьютера и информации?

Тест для закрепления материала

Этот тест поможет проверить знания начинающих пользователей Интернета. Большая часть этих вопросов размещена в сообществе «Ваш помощник Интернет»[3] в социальной сети «ВКонтакте», они оформлены с использованием сервиса Google Формы, поэтому их удобно использовать на занятиях.

1. Что наименее эффективно при защите почтового ящика от взлома?
— Открывать письма только от тех, кого вы знаете
— Никому не сообщать пароль, хранить его в недоступном для других месте
— Время от времени менять ящик электронной почты или провайдера
— Иметь отдельный пароль для каждого ящика и учетной записи

Правильный ответ: Время от времени менять ящик электронной почты или провайдера.

Комментарий: Это совершенно бессмысленно с точки зрения защиты своих данных, к тому же делает использование электронной почты крайне неудобным, ведь пришлось бы каждый раз сообщать новый адрес всем людям, с которыми вы переписываетесь. А вот соблюдать осторожность со входящими письмами и паролями очень важно.

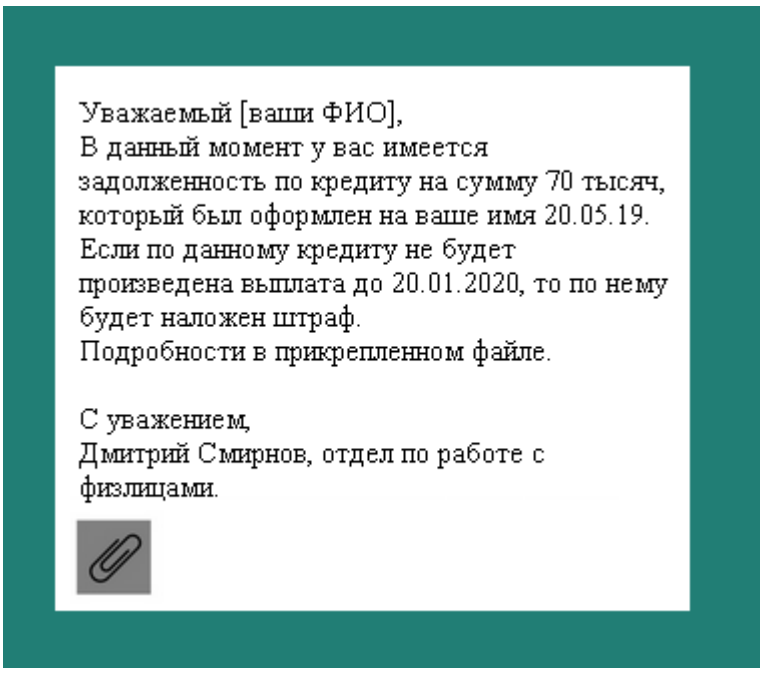
2. Какой пароль наиболее надежен?
— password483678
— vihodilanaberegkatyusha777
— a2a0t678t7658low

Правильный ответ: vihodilanaberegkatyusha777

Комментарий: Наиболее безопасен длинный пароль. Для запоминания также важно, чтобы пароль имел какое-либо персональное отношение к вам.

3. На ваш почтовый ящик пришло вот это письмо. Безопасно ли открывать вложение?

[3] Ваш помощник Интернет : курсы компьютерной грамотности для всех желающих : [группа] // ВКонтакте : российская социальная сеть. URL: https://vk.com/vashpom (дата обращения: 14.10.2020).

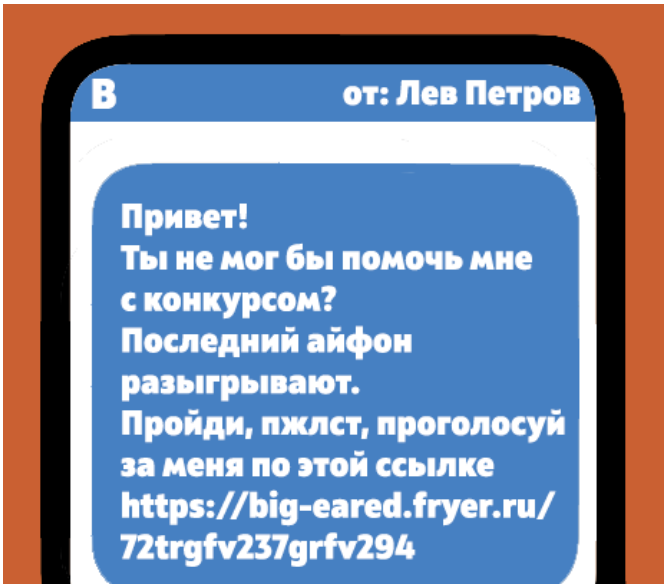


— Да.
— Нет.

Правильный ответ: Нет.

Комментарий: Вложения к письмам — это самый распространенный путь, по которому вирусы попадают на ваш компьютер. Эти вредоносные программы не только замедляют работу компьютера, их главная задача — фишинг. То есть они отправляют злоумышленникам ваши данные — номера карт, пароли, прочие реквизиты.

4. Вы получили от своего лучшего друга вот такое сообщение. Безопасно ли переходить по ссылке?



— Да.
— Нет.

Правильный ответ: Нет.

Комментарий: Аккаунт вашего друга могли взломать мошенники, а по ссылке расположить вредоносную программу. Чтобы убедиться, что это действительно ваш друг, вы можете задать ему вопрос, ответ на который знает только он, или связаться другим способом, например по телефону.

5. Какую информацию о себе можно безопасно сообщать при общении в Интернете или публиковать в открытом доступе?

— Место работы свое или знакомых
— Телефон или домашний адрес
— Информацию о своих хобби и интересах
— Дату рождения или полные ФИО

Правильный ответ: Информацию о своих хобби и интересах.

Комментарий: Место работы, телефон, домашний адрес и дата рождения позволяют легко определить вашу личность, найти вас в реальной жизни, данные также могут попасть в открытый доступ, тогда кто угодно сможет увидеть, например, ваш домашний адрес. По настоящему имени и дате рождения злоумышленники даже могут при должной сноровке вычислить ваши финансовые данные, данные вашего паспорта и других документов.

6. Вы просматриваете свою электронную почту. Какое из этих действий на сто процентов безопасно?

— Открывать письма, но не вложения
— Открывать письма только от знакомых людей
— Открывать только те письма и вложения, о которых заранее условились
— Проверять письма антивирусом
— Ничего

Правильный ответ: Открывать только те письма и вложения, о которых вы заранее условились.

Комментарий: Не только вложения, но и сами письма тоже могут быть опасны. Например, там могут быть ссылки, пройдя по которым вы также рискуете подхватить вирус или выдать свои личные данные мошенникам. Письма от знакомых людей не всегда безопасны, их почтовый ящик могут взломать.

7. Ваши частные электронные сообщения по почте и в мессенджерах не могут видеть посторонние?

— Да
— Нет

Правильный ответ: Нет.

Комментарий: Существуют программы, с помощью которых можно «видеть» вашу частную корреспонденцию, поэтому всегда убеждайтесь в надежности сайта, на котором вы общаетесь приватно.

8. Установленная однажды на компьютере антивирусная программа обезопасит его.

— Да
— Нет

Правильный ответ: Нет.

Комментарий: Простая установка антивируса поможет мало. Каждый день в Сети появляются новые вирусы, поэтому программу следует обновлять по крайней мере раз в месяц.

9. Можно ли с абсолютным доверием относиться к электронным сообщениям, которые вы получаете от своих друзей?

— Да
— Нет

Правильный ответ: Нет.

Комментарий: Вредоносные программы и вирусы могут рассылать сообщения каждому, кто есть в перечне адресатов вашей электронной почты. Точно так же и вы можете получить сообщение. Поэтому важно убедиться, что сообщение отправил именно ваш друг.

10. Что из перечисленного не стоит делать, когда вы придумываете надежный пароль?

— Использовать один и тот же пароль для нескольких аккаунтов
— Использовать генератор паролей, чтобы создать редкий пароль
— Использовать пароль длинною больше 6 символов
— Использовать числа, буквы и специальные символы

Правильный ответ: Использовать один и тот же пароль для нескольких аккаунтов.

Комментарий: Это опасно тем, что, подобрав пароль один раз, злоумышленник получает доступ сразу ко всем вашим интернет-регистрациям.

11. По какому признаку можно определить, что веб-сайт, который вы посещаете, имеет безопасное соединение?

— Необходимость ввести логин и пароль
— В адресной строке адрес начинается с https или есть логотип замка
— Нет рекламных баннеров

Правильный ответ: В адресной строке адрес начинается с https или есть изображение замка.

Комментарий: Это значит, что любые данные, которые вы наберете на этом сайте (ФИО, номер карты), будут зашифрованы, и злоумышленник вряд ли сможет их перехватить.

12. Когда безопасно использовать веб-камеру?

— Ее лучше никогда не использовать
— Для беседы с людьми, которых вы знаете в реальной жизни
— Для любых видеозвонков

Правильный ответ: Для беседы с людьми, которых вы знаете в реальной жизни.

Комментарий: Видеозвонки не всегда безопасны, записать транслируемое видео чрезвычайно легко.

13. Что делать, чтобы обеспечить безопасность веб-камеры?

— Регулярно обновлять антивирусную программу
— Убирать или закрывать веб-камеру, когда вы ею не пользуетесь

Правильный ответ: Убирать или закрывать веб-камеру, когда вы ею не пользуетесь.

Комментарий. Как вы уже знаете, существуют вирусы, способные незаметно для вас поставить вашу веб-камеру на запись и переслать эту запись злоумышленнику. Чтобы обезопасить себя от этого, закрывайте неиспользуемую камеру и, конечно, не открывайте посланные вам по почте и соцсетям файлы неизвестного происхождения (в них и находятся эти вирусы).

14. Вы получили по электронной почте письмо с неизвестного адреса. В нем говорится, что вы выиграли в лотерею. Для того чтобы обналичить деньги, вам нужно открыть вложение. Как стоит поступить в такой ситуации?

— Открыть вложение и обналичить выигрыш
— Отметить сообщение как спам, не открывая вложение
— Связаться с отправителем для уточнения деталей
— Поискать информацию об отправителе через поисковые системы, а потом принять решение

Правильный ответ: Отметить сообщение как спам, не открывая вложение.

Комментарий: Ни в коем случае не открывайте ссылки и вложения в письмах, пришедших с неизвестных адресов. Ссылки могут оказаться мошенническими, а вложения — содержать вирусы. Если вы не участвовали в лотерее, но получили письмо, сразу отметьте его как спам. Если участвовали, зайдите на официальный сайт лотереи и проверьте информацию из письма.

15. Как нужно поступить, если ваш друг оказался в беде и просит вас в личном сообщении в социальной сети одолжить ему денег, пополнив счет мобильного телефона?

— Написать ему вопрос: «Что случилось?»
— Задать вопрос, ответ на который знаете только вы и он
— Незамедлительно помочь
— Позвонить ему, предложить встретиться и отдать деньги наличными

Правильный ответ: Позвонить ему, предложить встретиться и отдать деньги наличными.

Комментарий. Ни в коем случае не переводите деньги, пока не убедитесь, что вам пишет именно ваш друг. Может оказаться, что его страница взломана и вам пишут мошенники с целью наживы. Единственно верным решением будет позвонить ему и договориться о личной встрече.

16. Как невозможно подхватить вирус?

— Нажав на сайте броский заголовок статьи.
— Перейдя по ссылке, которую прислал друг.
— Зайдя в незнакомое приложение в соцсети «ВКонтакте».
— Нет верного ответа.

Правильный ответ: Нет верного ответа.

Комментарий. В каждом из этих случаев мы становимся уязвимы перед злоумышленниками. Опасны сообщения, незнакомые сайты и программы, подхватить вирус можно и через статью со скандальным заголовком и даже через просмотр сериала на пиратском сайте.