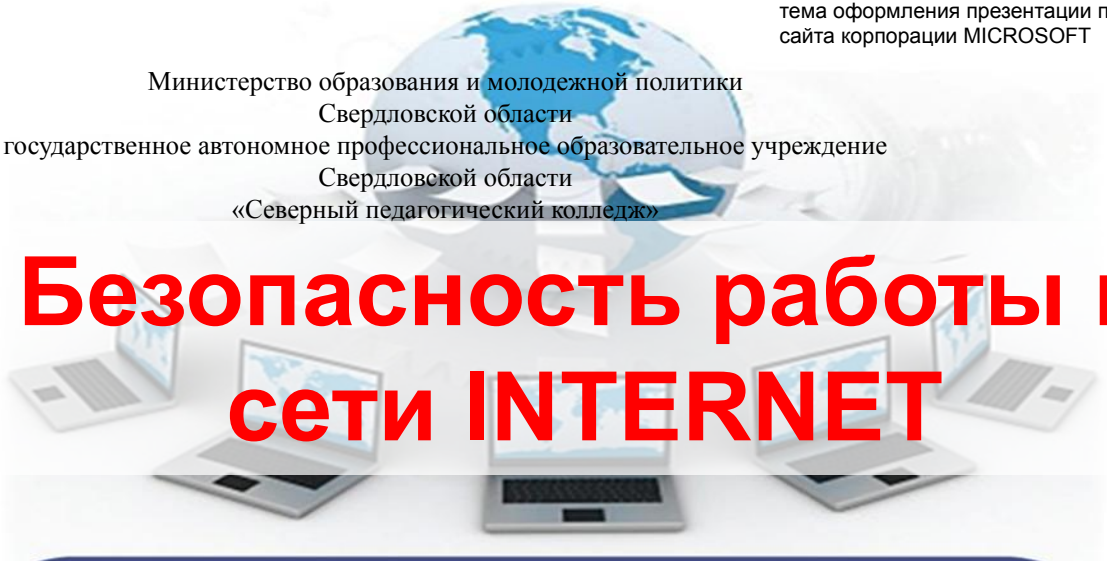
тема оформления презентации позаимствована с официального сайта корпорации MICROSOFT

Министерство образования и молодежной политики
Свердловской области
государственное автономное профессиональное образовательное учреждение
Свердловской области
«Северный педагогический колледж»



Безопасность работы в сети INTERNET

Коллективная презентация
148 группы
март 2023

Возможные опасности сети INTERNET

Дудко Ляна

Опасности сети Интернет

Мы уже привыкли к тому, что пропускаем за день огромные потоки информации. Мы давно стали Цезарями: параллельно работаем, переписываемся, читаем, смотрим, комментируем, бродим по сайтам, перелопачивая тонны контента как нужного, так и не очень.

Основными техническими угрозами для пользователей являются вредоносные программы:

- **Ботнеты**
- **DoS - атака**
- **DDoS - атака**

1. Источник информации
2. Источник информации

Что такое СПАМ и как с ним бороться?

Давыдов Андрей

Спам – это массовая рассылка рекламных писем пользователям, которые не давали на это своего согласия.

1.Главный совет, который не раз показывал свою эффективность: **зарегистрируйте хотя бы два электронных адреса.** Один для личных и рабочих контактов, а второй для регистрации на коммерческих сайтах, сайтах с сомнительным содержимым.

2.Следующий совет –**выбирайте надежный почтовый сервис.**

3.Также для избавления от спама можно **использовать фильтры и создавать правила.**

4.Если какое-то письмо все-таки «прорвалось» в основную папку с письмами, обязательно **отмечайте его как спам**– все дальнейшие письма от этого пользователя попадут туда же.

https://timeweb.com/ru/community/articles/chto-takoe-spam-i-kak-s-nim-borotsya-1

Кто такие ХАКЕРЫ и как от них защититься?

Союрова Елена

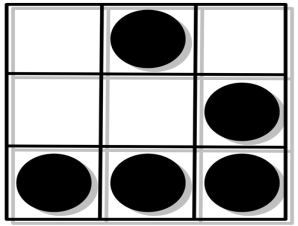
Хакер-это специалист в области информационных технологий, который использует свои технические знания для достижения цели или преодоления препятствия в рамках компьютеризированной системы нестандартными средствами.

Как обезопасить себя от хакеров?

Главным способом защиты от хакеров будет предотвращение их действий. Для этого не стоит переходить на подозрительные сайты и скачивать файлы или данные из подозрительных источников, поскольку, таким образом удается минимизировать риск заражения компьютера или потери личных данных. Использование современных антивирусов с актуальными базами данных приложений. При этом, не рекомендуется использовать бесплатные программы, которые не обеспечивают достаточную эффективность защиты, например Avast или Avira. Хотя, согласно данным немецкого агентства исследования эффективности, бесплатный антивирус Windows Defender является сравнимым по эффективности с лучшими представителями платных систем. Быть аккуратнее в общении в сети, в особенности с малознакомыми или незнакомыми людьми, которые могут применить различные методы социальной инженерии для получения доступа к личным данным. Не допускать утечки личных данных. Оплачивайте покупки в интернете виртуальной картой, либо другим безопасным методом, не допускайте отправки паспортных данных или личной информации в непроверенные источники.

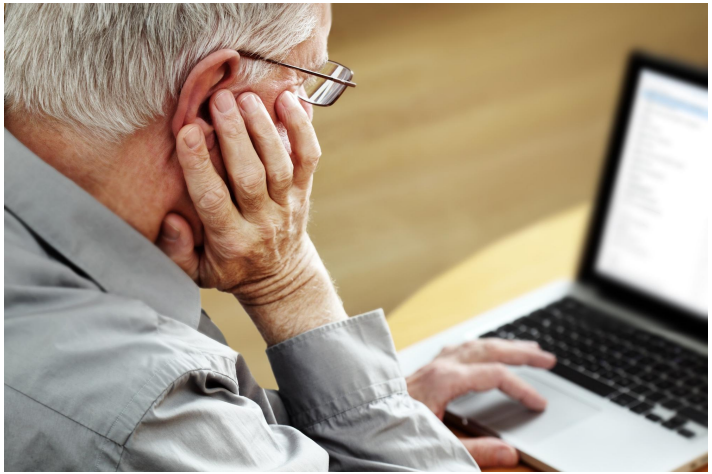
1.https://itstan.ru/programmirovanie/kto-takoy-haker.html
2.https://en.wikipedia.org/wiki/Hacker

эмблема хакеров -



Правила пользования интернетом для пожилых людей

Карпасов Дмитрий



1. Не доверяйте каждому письму, которое Вы получили.

2. Используйте различные пароли и регулярно меняйте их.

3.Установите антивирус на все Ваши устройства.

4.Удаляйте следы Вашего пребывания, если Вы работаете на чужом компьютере.

5.Пользуйтесь Ad блоком для защиты от назойливой рекламы.

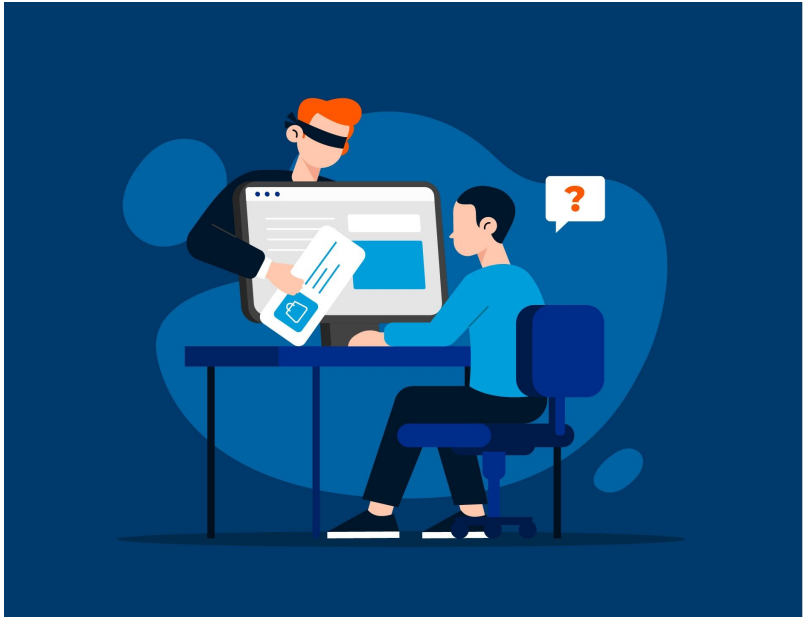
Тест:
https://onlinetestpad.com/ru/testresult/140841-bezopasnost-v-seti-internet?res=dzs3sfa5h3eve

Что такое фишинг?

Силкина Алина

Фишинг — это распространенный способ интернет-мошенничества. Хакеры используют его, чтобы получить доступ к конфиденциальной информации других людей: их учетным записям и данным банковских карт.

Фишинговые мошенники действуют по отработанной схеме: закидывают «наживку» — письмо, сообщение, ссылку на сайт — и пытаются «поймать» доверчивых пользователей. Поэтому неудивительно, что сам термин произошел от англоязычного phishing, которое созвучно со словом fishing — «рыбалка». Замена f на ph — отсылка к оригинальной форме хакерства фрикингу, или телефонному взлому (phreaking).



Источник : https://www.unisender.com/ru/glossary/chto-takoe-fishing-i-kak-ot-nego-zashchititsya/

Почему нужно избегать знакомств в интернете?

Егорова Марина

Разные люди фотогеничны по-разному. Кто-то получается лучше, чем в жизни, а кто-то сам на себя не похож. Многие, подчиняясь естественному желанию привлечь внимание, увлекаются фотошопом.

Чаще всего при первом знакомстве в виртуальном мире мы не слышим приветствующего нас голоса, не чувствуем запаха нового знакомца. А возможность тщательно продумать и проработать внешний вид своей страницы лишает нас возможности увидеть человека в момент импровизации.

Опять же переписка дает больше шансов продумать фразу, лишая виртуальную беседу некой спонтанности и, вместе с тем, естественности.

Чем опасны азартные игры в Internet?

Дуденков Глеб

Казино, Ставки и многии другии азартные игры заполняют добрую часть интернета. Чем они могут быть опасны ?...

Банально но и в тоже время очевидно они опасны появлением зависимости.

Лудомания (с латинского "лудо" – играю, "мания" – влечение, страсть) – неконтролируемое человеком патологическое пристрастие к различным азартным играм (игровые автоматы, реальные и онлайн-казино и т. п.).

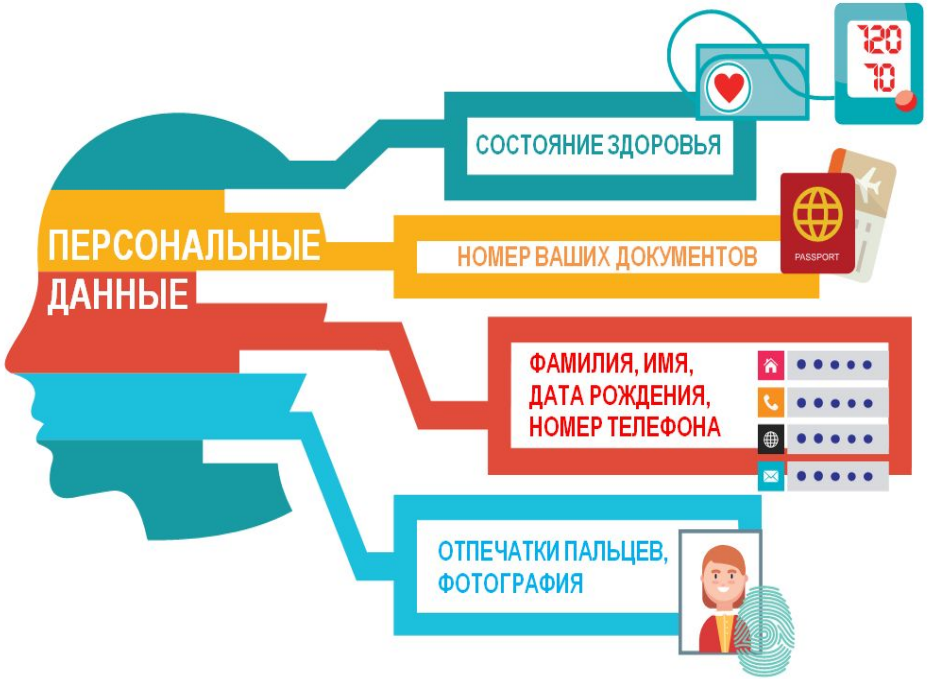
Именна эта болезнь таит опасность азартных игр.

Сыграв один раз и выиграл “ставку” мы начинаем думать что это реальный способ заработать деньги. Но не успев оглянуться игрок понимает что он попал в ловушку.

В частности очень распространено что казино дает заведомо победу новому игроку чтобы поймать его на крючок и не понимает того сам игрок начинает уходить в убытки и терять большие суммы надеясь отыграться.

Какие данные относятся к персональным? Молозинова Анна

Персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)



https://www.consultant.ru/document/cons_doc_LAW_61801/4f41fe599ce341751e4e34dc50a4b676674c1416/

Что такое кибератака и как от нее уберечься?

Колягина Евгения

Кибератака - это угроза вашей личной или корпоративной безопасности, исходящая от неизвестных анонимных злоумышленников в сети, с целью их обогащения или иного профита и с плохо прогнозируемыми потерями для вас. Производится разными методами, носит различный характер и не имеет чёткой схемы избегания, поэтому придётся немного погрузиться в вопрос.

Чтобы уберечь себя от кибератак, нужно делать следующее:

- Регулярно обновляйте операционные системы устройств и мобильные приложения.
- С подозрением относитесь к сообщениям от незнакомых отправителей, особенно к тем, которые содержат ссылки или вложения.
- Не нажимайте на подозрительные ссылки или подозрительные электронные письма и вложения.
- Проверяйте URL-адреса, прежде чем переходить по ссылкам, или переходите на веб-сайты напрямую.
- Регулярно перезагружайте мобильные устройства, что может помочь повредить компоненты вредоносных программ.
- Используйте шифрование и защищайте паролем ваши устройства.
- По возможности сохраняйте физический контроль над своим устройством.
- Используйте VPN.

https://www.podolsk.ru/news-club/n37449.html
https://www.ferra.ru/news/techlife/kak-zashitit-sebya-ot-kiberatak-07-01-2022.htm

Зачем нужен злоумышленникам доступ к компьютеру пользователя?

Дежурова Ирина

Это раньше хакеры часто писали вирусы просто ради интереса, сейчас же это делается почти всегда с коммерческой выгодой. Лет 20 тому назад злоумышленник получал удовольствие от того, что мог просто отформатировать жесткий диск. Или сделать так, что при включении компьютера вместо стандартного рабочего стола появятся какие-либо прикольные картинки. Сейчас же они делают все возможное, чтобы владелец ПК как можно дольше не знал о том, что его устройство заражено и втайне от него выполняет дополнительные функции.

Кроме того, о чем было сказано выше, хакеры стараются получить доступ к вашим электронным почтам, кошелькам, аккаунтам в социальных сетях, форумах.

Пять правил для родителей, которые заинтересованы в безопасности своих детей в интернете.

Приходько Ульяна

В наши дни мы все проводим много времени в интернете, в том числе дети и подростки. Каждый родитель хочет, чтобы дети чувствовали себя в безопасности, находясь в сети, ведь в интернете есть вещи, которых следует опасаться. Свод некоторых правил, которые могут уберечь детей:

1. Стройте открытые и доверительные отношения с ребенком
2. Больше времени проводите вместе с ребенком в реальной жизни.
3. Используйте устройства в хорошо просматриваемом месте в доме
4. Установите ограничения по времени пользования электронных устройств, особенно в ночное время.
5. Обращайте внимание на настроение и поведение ребенка.