Правила безопасного поведения в интернете

(классические советы читателям)

«Дело помощи утопающим – дело рук самих утопающих…»

Цифровой мир – это пространство информации, знаний и возможностей, но он полон рисков и угроз

Чтобы безопасно и эффективно использовать виртуальные технологии и ресурсы интернета, защитить себя, свои персональные данные и цифровые устройства, необходимо сформировать полезные привычки и выполнять определенные правила.

"Привычка свыше нам дана:
Замена счастию она..."

Поделитесь этими советами со своими близкими!

- «Фишинг» (от англ. phishing (рыбачить) — это попытка злоумышленников «выудить» личные данные пользователей. Внимательно проверяйте адреса ссылок, логотипы, текст и отправителя сообщений. Фишинговые ссылки обычно похожи на адреса популярных ресурсов.

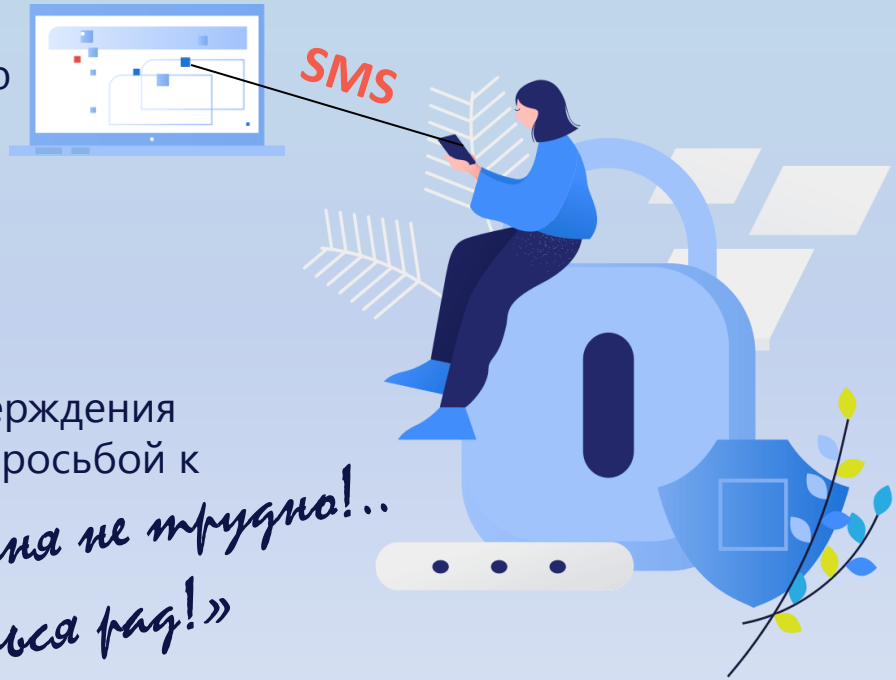
Не попадитесь на «удочку» кибер-мошенников!

«Гений и злодейство – две вещи несовместные...» (увы!!!)

- Не переходите по ссылкам, пришедшим в сообщениях от непроверенных отправителей. Это верный способ заразить свое устройство вредоносными программами.
- Если вас взломали, то необходимо предупредить об этом всех своих виртуальных знакомых, возможно, от вашего имени будет рассылаться спам и ссылки на фишинговые сайты.

Берегите доступ!

- Везде, где это возможно, активируйте двухфакторную аутентификацию, то есть такую систему доступа, которая основана на двух «ключах»: одним вы владеете (телефон, на который приходит вызов или SMS с кодом подтверждения), другой – запоминаете (обычные логин и пароль).



- Никому и никогда не отправляйте коды подтверждения из смс-сообщений, с какой бы убедительной просьбой к вам не обращались.

«Ах, обмануть меня не трудно!..
Я сам обманываться рад!»

- Поставьте PIN на блокировку своего смартфона. Не помогайте зарабатывать карманникам!

Пароль – под контроль!

Пароль – главный авторизационный механизм в интернете,
но этот механизм небезупречен.

- Не используйте один и тот же пароль для нескольких сервисов или учетных записей. Всего одна утечка – и все ваши аккаунты будут под угрозой.
- Суперважный пароль – пароль для входа в основную электронную почту. Он дает возможность воспользоваться функцией восстановления паролей для всех привязанных к нему аккаунтов и сервисов.
  Лучше сделать его совершенно непохожим на все остальные.
- Постоянно менять пароли — не очень эффективно. Лучше использовать уникальные и в то же время запоминающиеся пароли.

«Береги честь смолоду!» (и пароль!)

Один из способов создавать и запоминать надежные пароли:

Придумайте длинную комбинацию. Чем длиннее, тем лучше.

Используйте как можно более разнообразные символы.

Чтобы легко запомнить такую последовательность, придумайте её на базе фразы, которая что-то для вас значит: строка из песни, цитата из фильма, детская колыбельная...

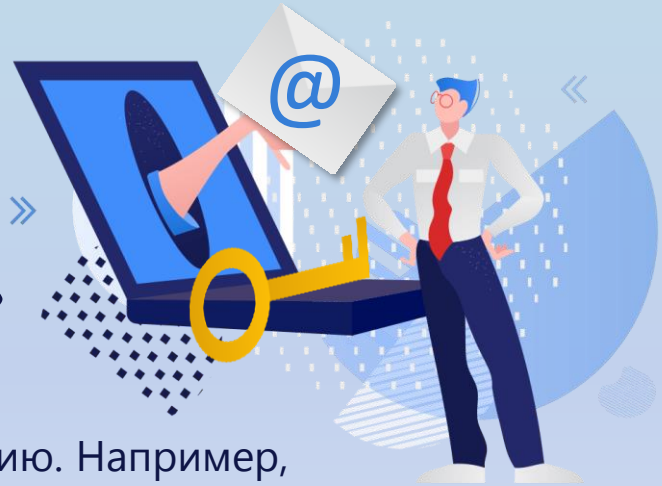
Запишите первые буквы из первых пяти слов.
Добавьте специальные символы между буквами.

Это базовая комбинация.

Используя различные ассоциации, дополняйте её, и вы сможете сочинить бесконечное количество уникальных паролей для ваших аккаунтов.

«Тройка, семерка, туз...»

- Создайте несколько адресов электронной почты: основную, для онлайн-покупок и развлекательную (для извещений из социальных сетей, форумов, подписок и пр.).
- Не храните в электронном почтовом ящике ценную информацию, секретные документы и интимные фотографии.



Почта – ключ ко всему!

«Я к вам пишу – чего же боле?»

- Не указывайте в адресе почты персональную информацию. Например, лучше выбрать «jazz_forever@» или «rock13@» вместо «temaivanov2001@»
- Не отвечайте на спам и не переходите по указанным в нем ссылкам!
- Помните, банки или платежные системы НИКОГДА не запрашивают конфиденциальную информацию по электронной почте.
- После окончания работы в почтовом сервисе перед закрытием вкладки с сайтом не забудьте нажать на «Выйти».

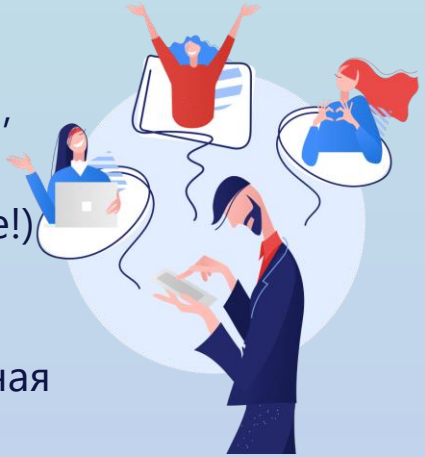
- Не всем интернет-магазинам можно доверять. Изучайте отзывы реальных покупателей. Обращайте внимание на внешний вид сайта.
- Помните, адрес защищенной страницы, с которой можно проводить платеж, должен начинаться с «https://» и иметь пиктограмму в виде закрытого замка зеленого цвета.

Платите и покупайте безопасно!

«Может быть, тебе дать еще ключ от квартиры, где деньги лежат?»

- Не проводите финансовые операции через открытые Wi-Fi-сети в кафе или на улице.
- Заведите отдельную (можно виртуальную) карту для платежей в интернете.
- Не пренебрегайте возможностью услуги «смс-оповещение» от банка.

- Будьте осторожны при общении в сети с незнакомцами, они могут оказаться не теми, за кого себя выдают.
- Не выкладывайте в сеть (а лучше не делайте!) фотографии и видео, которые могут вас скомпрометировать. Следите за тем, чтобы в кадр случайно не попала конфиденциальная информация.



Дорожите цифровой репутацией!

- Помните, что за вашим поведением в соцсетях могут следить конкуренты и работодатели. Прежде чем хвалиться рабочими достижениями, подумайте, не являются ли они коммерческой или корпоративной тайной.

- Не публикуйте в сети домашний адрес, документы... Не сообщайте о своем отъезде, о том, в какое время вас не бывает дома. Не хвалитесь крупными покупками и вообще постарайтесь не афишировать уровень достатка.

«...Как будто нам уж невозможно
Писать поэмы о другом,
Как только о себе самом...»

«Кликайте на добро!»

- Общаясь виртуально, придерживайтесь тех же нравственных норм, что и в жизни. Будьте взаимно вежливы, не нарушайте чужих личных границ и не позволяйте нарушать свои.

- Кибербуллинг (унижение и травля в цифровой среде) и троллинг (агрессивные, оскорбительные или провокационные комментарии в социальных сетях) – отвратительные явления.

Умейте противостоять им:

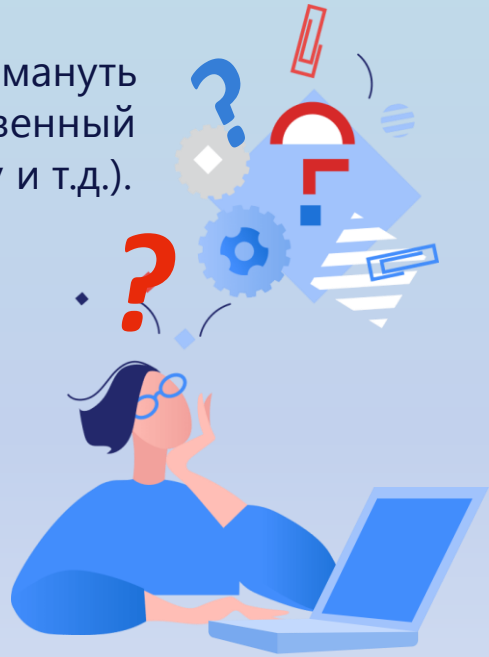
- не пытайтесь ответить обидчику тем же, не оправдывайтесь, игнорируйте его;

- расскажите о ситуации человеку, которому вы доверяете;

- настройте достаточный уровень приватности в социальных сетях. Используйте инструменты онлайн-платформ для блокировки, обеспечения собственной безопасности и комфортного общения.

«Ах! Злые языки страшнее пистолета...»

Осторожно, фейки!



Фейк – это нечто ложное, ненастоящее, поддельное. Созданное, чтобы обмануть вас (с различной целью: испортить чью-то репутацию, продать некачественный товар, посеять панику, обострить общественно-политическую обстановку и т.д.).
В интернете фейки встречаются на каждом шагу.

Не позволяйте манипулировать собой!

- Мыслите критически, рассуждайте логически, делайте выводы, основанные на фактах!
- Проверяйте достоверность информации:
  - сравнивайте данные из разных авторитетных источников;
  - устанавливайте авторство публикации (текста, фотографии, видео);
  - обращайте внимание на форму подачи информации: нет ли излишней эмоциональности, грубых ошибок, неточностей, несоответствий.
- Не распространяйте информацию сразу после её публикации.

«Кого же любить?
Кому же верить?»

Полезные ссылки

Посмотреть обучающие ролики и статьи, узнать подробнее о том, как не стать жертвой мошенников в интернете, как сделать свою цифровую жизнь безопасной и комфортной, можно здесь:

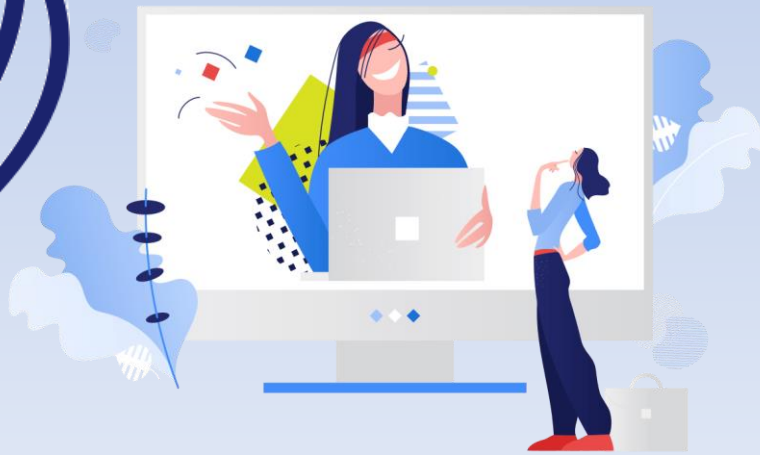
Портал «Цифровая грамотность»

Блог Касперского

Центр интернет-технологий (РОЦИТ)

Цифровой диктант.РФ

«Мы все учились понемногу…»



Что читать в Пушкинке

Колисниченко, Д.Н. Анонимность и безопасность в Интернете. От "чайника" к пользователю / Д.Н. Колисниченко. – Санкт-Петербург : BHV, 2012. – 240 с.: ил. – (Самоучитель).

Мельников, В.П. Информационная безопасность : учебник / В.П. Мельников, А.И. Куприянов, Т.Ю. Васильева ; под ред. В.П. Мельникова. – Москва : КНОРУС, 2017. – 372 с. – Текст : электронный // ЛитРес : электронная библиотечная система : [сайт]. – URL: https://biblio.litres.ru/aleksandr-kupriyanov-12189829/informacionnaya-bezopasnost-29804638/ (дата обращения 09.11.2020). – Режим доступа: для зарегистрированных пользователей ККУНБ им. А.С. Пушкина.

«Читай не так, как пономарь,
А с чувством, с толком, с расстановкой»

Жвалевский, А. Интернет без напряга / А. Жвалевский, Г. Кондратьев. – 2-е изд. – Санкт-Петербург : Питер, 2011. – 336 с.: ил. – (Без напряга).

Левин, Дж. Интернет для чайников / Дж. Левин, М. Левин. – Москва : Диалектика, 2011. – 352 с.: ил.

Пастернак, Е. Б. Интернет для женщин / Е. Б. Пастернак. – 2-е изд. – Санкт-Петербург : Питер, 2011. – 256 с.: ил.

Шунейко А. А., Авдеенко И. А. Информационная безопасность человека : Учебное пособие для вузов / А.А. Шунейко, И.А. Авдеенко. – Москва : ВЛАДОС, 2018. – 177 с. – Текст : электронный // БиблиоРоссика : электронная библиотечная система : [сайт]. – URL: http://www.bibliorossica.com/book.html?currBookId=26414 (дата обращения 09.11.2020). – Режим доступа: для зарегистрированных пользователей ККУНБ им. А.С. Пушкина.

Уважаемые читатели!

В центре правовой информации и электронных ресурсов Краснодарской краевой универсальной научной библиотеки имени А.С. Пушкина можно узнать об основах безопасного поведения в цифровой среде, обеспечении конфиденциальности, о наиболее типичных угрозах при работе в сети Интернет.

Телефон: 8 (861) 268-15-87

E-meil: echz@pushkin.kubannet.ru

VK Ig FB

Библиотека – ваш цифровой куратор!

«Приятны завершенные труды»

Презентация подготовлена с использованием
векторных иллюстраций icons8

ГБУК КК «Краснодарская краевая универсальная
научная библиотека им. А.С. Пушкина»
Центр правовой информации и электронных ресурсов
г. Краснодар
2020 г.