

‘ЗАКРЫВАЙТЕ’ ONLINE

Вы закрываете свой дом, машину, ценности... Закрываете online?

Интернет - удивительная вещь. Мир широко открыт для вас от шопинга до общения. Задумайтесь, вы бы дали незнакомцу свою банковскую карточку с пинкодом, свой компьютер или оставили бы открытой свою входную дверь?

‘Закройте online’ и перекройте доступ интернет-вору в ваш мир. Прочитайте наши советы, чтобы не стать жертвой виртуального преследования.



‘ЗАКРЫВАЙТЕ’
ONLINE

Слесари

Для дополнительной информации зайдите на:
www.derby.gov.uk/lockuponline

Заявите о мошенничестве: www.actionfraud.org.uk
Дополнительная информация: www.getsafeonline.org.uk
Пользуйтесь банком безопасно: www.banksafeonline.org.uk
Заявите о содержании уголовного характера: www.iwt.org.uk

Дополнительная информация о безопасности ребёнка online.
www.childnet-int.org или www.ceop.police.uk

CYBER CRIME
www.derby.gov.uk/lockuponline



Join us on Facebook
[Facebook/derbycc](https://www.facebook.com/derbycc)
[Facebook/SaferDerbyCity](https://www.facebook.com/SaferDerbyCity)



Follow us on Twitter
[@DerbyCC](https://twitter.com/DerbyCC)
[@SaferDerbyCity](https://twitter.com/SaferDerbyCity)



Derby City Council

‘Запирайтесь’ на ходу

Не позволяйте своему смартфону или планшету попасть в руки интернет-вора. ‘Запирайтесь’ на ходу.



- Не оставляйте его на виду в открытой сумке, на сиденьях или на видном месте в своей машине.
- Сделайте отметку на своём телефоне с УФ ручкой и зарегистрируйтесь на сайте www.immobilise.com
- Используйте пароль или PIN, чтобы заблокировать ваш телефон
- Запишите номер IMEI, который вы можете найти на батарее телефона или корпусе для SIM карты. Также его можно определить, набрав *#06#
- Ограничьте использование альтернативной сети. Незащищённый паролем Wi-Fi не только является риском, но и разряжает батарею вашего телефона.
- Постарайтесь не оставлять включенным ваш bluetooth, защитите его паролем.
- Убедитесь, что вы знаете какие данные сохранены у вас в телефоне, когда подсоединяете телефон к компьютеру.
- Регулярно подсоединяйте свой телефон к компьютеру.



Определяйте МОШЕННИЧЕСТВО

Интернет-воры любят аферы с зарабатыванием денег. Будьте на шаг вперёд – определяйте мошенничество.

Разновидности мошенничества и важные советы:

Ложные вебсайты

- Будьте осторожны, когда покупаете билеты и путёвки online
- Пользуйтесь только сайтами с хорошей репутацией
- Изучите сайт и проверьте отзывы о нём.

Ложные электронные письма

- Если вы не уверены от кого вы получили электронное письмо, не открывайте его, не нажимайте ни на какие ссылки
- Никогда не отвечайте на электронное письмо, с запросом денег или личных данных, даже если оно пришло от вашего друга
- Не отвечайте на письма с угрозами.

Сайты аукционов

- Внимательно читайте описание вещи
- Проверьте последние отзывы и задайте вопросы
- Оставьте свой отзыв
- Обратитесь за дополнительной информацией, сайты аукционов могут проконсультировать вас насчёт безопасности
- Не торопитесь ставить ставки или покупать вещи
- Не ставьте ставки выше, чем вы намеревались поставить
- Не гадайте и не делайте предположений.

Рекламирование

- Знайте, что вы можете оказаться целью, если вы только что объявили на Facebook, что обручены, вдруг у вас будет появляться реклама, связанная с темой свадьбы
- Не подписывайтесь к чему-то, чего вы не хотите
- Не поддавайтесь на обещания бесплатных вещей или ложных призов.

Разбогатеете быстро

- Держитесь от этого подальше, почти всегда это сделает вас беднее, а не богаче.



'Закройтесь' и сделайте резервное копирование

Закройте доступ интернет-вору в свой компьютер и в свой мир. 'Закройтесь' и сделайте резервное копирование.

Советы о паролях

- Не используйте один и тот же пароль везде
- При смене пароля используйте что-то совершенно непохожее на предыдущий пароль
- Не храните свой пароль рядом с компьютером или в компьютере
- Не нажимайте 'запомнить пароль'
- Избегайте использование дней рождений/ годовщин/ кличек домашних животных/ футбольных команд и т.д.
- Используйте маленькие и заглавные буквы, а также числа и символы.

Советы

- Используйте антивирусную программу, и убедитесь, что вы защищены
- Всегда скачивайте обновления
- Проверьте, поставлен ли у вас пароль при включении компьютера
- Не заходите в свою личную информацию, используя бесплатный и небезопасный Wi-Fi
- Всегда обезопасьте свой Wi-Fi надёжным паролем
- Сделайте резервное копирование, используя CD диск, hard-drive жёсткий диск или USB флэшку
- Поставьте код на USB флэшку
- Проверяйте firewalls. Есть много бесплатных и доступных для скачивания online
- Не храните личную информацию в документах или на листах около компьютера.



Закройте свою ЖИЗНЬ

интернет-вора много лиц, не позволяйте воспользоваться вами, а также не пускайте нежелательных 'друзей' в ваш мир массовой информации. 'Закройте' свою жизнь!

Средства массовой информации

Facebook, YouTube и Twitter являются частью повседневной жизни. Будьте осторожны, то, что вы пишете в интернете, может быть использовано мошенниками против вас.

- Если бы на улице к вам подошёл незнакомец и спросил у вас какую-либо личную информацию, вы бы сказали ему? Если ваш ответ нет, не пишите это и online
- Узнайте больше о личных настройках и делитесь только тем, чем хотите делиться
- Заявляйте о нарушении конфиденциальности
- Объясните своим детям о рисках общения в социальных сетях, включая online chat rooms, online игры, или о том, чего не следует нажимать
- Знайте, что у игр и apps бывают скрытые расходы, смотрите чтобы большой счёт вас не ужалил
- Узнайте больше о защите пароля и родительском контроле.

Интернет магазин

- Хорошая ли репутация у вебсайта?
- Когда вы делаете платёж, появляется ли значок безопасности, обычно замочек справа внизу на экране или в графе с адресом?
- Может сделка слишком хороша, чтобы оказаться правдой?
- Вебсайт кажется вам каким-то необычным?
- Процесс платежа показался странным?

Вы можете заявить в государственный центр Великобритании по отчётности о мошенничестве www.actionfraud.org.uk

Интернет банк

- Внимательно посмотрите на вебсайт, если он не кажется вам правильным, наверное так оно и есть
- Не записывайте и не оставляйте банковские пароли у компьютера
- Будьте осторожны, получив электронную почту, утверждающую, что она из вашего банка. Не нажимайте ни на какие ссылки и не давайте свои банковские детали
- Иногда ваш банк может вам помочь, если образовалась какая-то проблема - действуйте быстро.