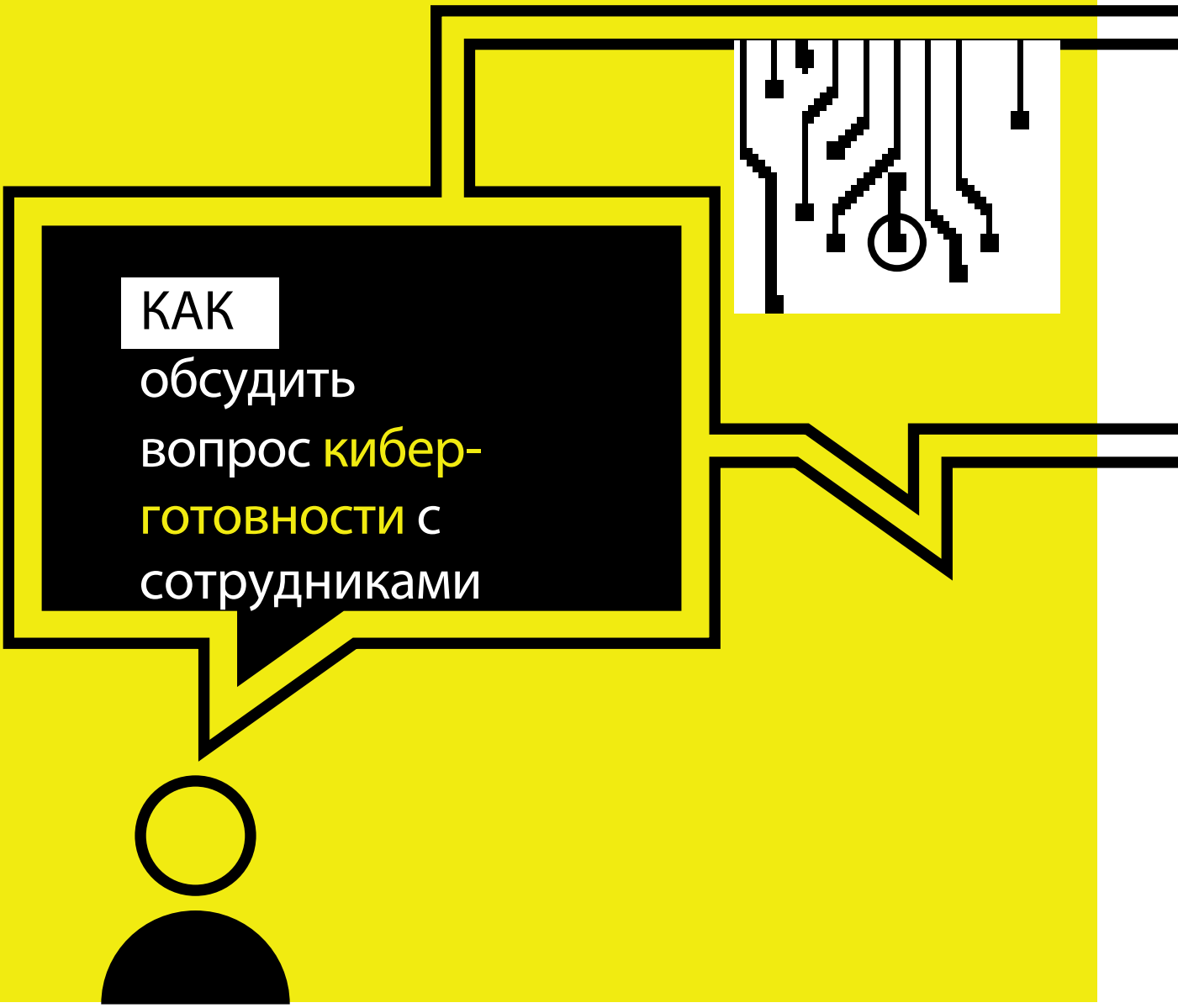
CYBER READINESS
INSTITUTE

Время поговорить



Важно СЕРЬЕЗНО относиться к вопросу о киберготовности.

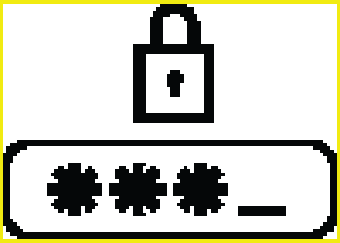
От этого зависит репутация вашего бизнеса.

НО КАК НАЧАТЬ РАЗГОВОР, ЕСЛИ ВЫ НЕ КИБЕРЭКСПЕРТ?

Он не должен быть сложным или пугающим. Прочитайте вопросы и ответы в этом документе, чтобы поговорить со своими сотрудниками о киберрисках, средствах защиты и передовых методах киберготовности.

— 1 —

Пароли

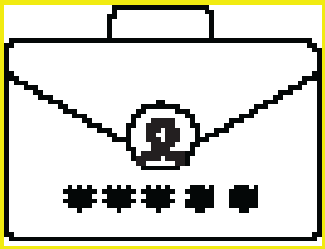


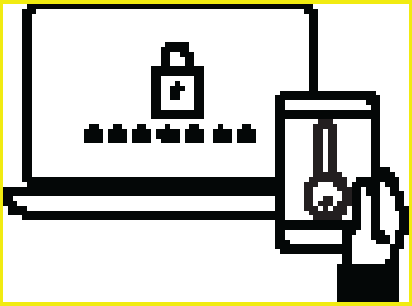
Какие пароли являются самыми надежными?

Самые надежные пароли — это парольные фразы: случайные мысли, которые образуют предложение. Парольная фраза должна включать не менее 15 символов.

Следует ли использовать один и тот же пароль для деловых и личных целей?

Нет, по возможности не используйте одни и те же пароли.



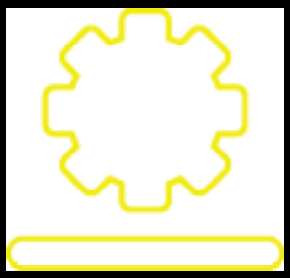


Что такое двухфакторная аутентификация?

Двухфакторная аутентификация — это способ подтверждения вашей личности с помощью пароля, а также другого метода такого, как текстовое сообщение или электронная почта. Двухфакторная аутентификация проста в настройке и значительно снижает ваши шансы на взлом.

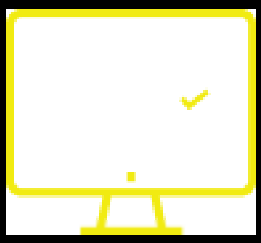
— 2 —

Обновления



Что такое обновления?

Если говорить простым языком, «обновления» — это новые версии программного обеспечения и приложений на вашем телефоне и компьютере. Обновления устраняют проблемы и повышают уровень безопасности. Установка обновлений — одна из самых простых и важных мер по киберготовности, которую вы можете предпринять.

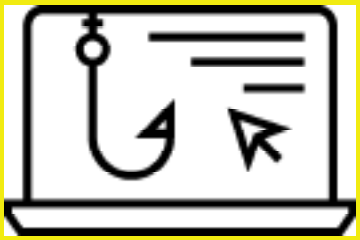


Как вы можете убедиться, что ваши устройства обновлены?

Включите уведомления об автоматических обновлениях и не игнорируйте уведомления о них. Также не забывайте проверять сторонние приложения на наличие обновлений.

— 3 —

Фишинг

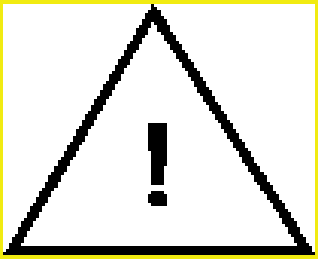


Что такое фишинг?

Фишинг — это кибератака, осуществляемая через фальшивое электронное письмо. Фишинговые атаки пытаются использовать вашу учетную запись для кражи личных данных или захвата вашего компьютера. Эти атаки часто трудно обнаружить.

Каковы общие признаки попытки фишинга?

Подозрительный адрес электронной почты
Письма от незнакомцев с вложениями или ссылками
Орфографические ошибки или неразборчивые предложения
Подозрительные электронные письма, в которых запрашиваются личные данные

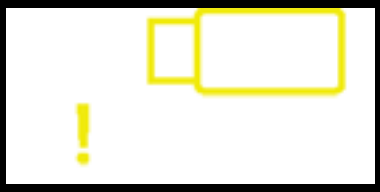


Почему так важно знать о рисках фишинга?

91% всех кибератак начинаются с фишингового письма.
81% компаний, попавших под фишинговую атаку, теряют клиентов.

— 4 —

USB-накопители



Что плохого в USB-накопителях?

Более четверти случаев заражения вредоносным ПО начинаются с зараженного USB-накопителя. Более того, 87% сотрудников говорят о потере USB-накопителя и не сообщают об этом своим работодателям.

Как можно ограничить USB-атаки?

Не использовать
USB-накопители, если они не одобрены вашим специалистом по киберготовности

Никогда не использовать
или принимать USB-накопители от стороннего лица или сторонней компании

При использовании
USB-накопителей их следует регулярно проверять на наличие вредоносных программ

CYBER READINESS
INSTITUTE