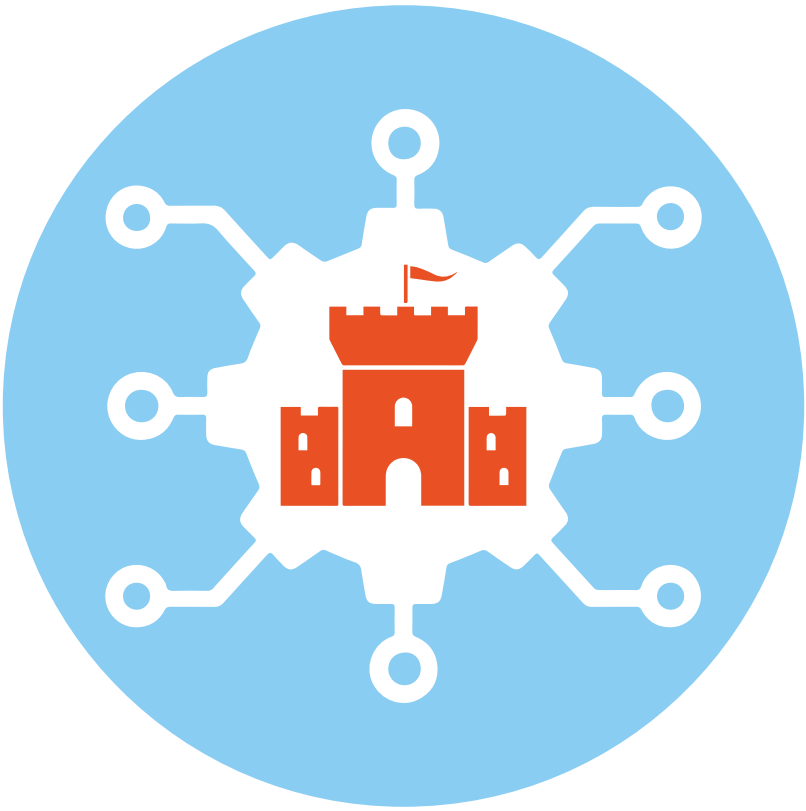

Глава 11

Строим цифровую крепость

Заключительная глава,
в которой мы вспомним все полезные советы
и, закончив чтение, тут же начнем применять
их на практике.

В интернете действует то же правило, что и в самолете, — сначала обеспечьте безопасность себе, потом ребенку. То есть взрослым нужно самим освоить правила кибербезопасности и понимать природу разнообразных цифровых угроз, чтобы стать для своего ребенка авторитетом. И, разумеется, разговоры надо подкреплять личным примером.

> *Помните: на одних запретах далеко не уедешь. Дети обязательно найдут способ вырваться за очерченный взрослыми периметр, и если основы безопасного поведения в онлайн-среде не заложены у них в голове, то велик риск того, что они попадут в какую-нибудь опасную ситуацию.*

Еще одна важная вещь: не стесняйтесь спрашивать и учиться у своих детей. В этом цифровом мире мы все новички, поэтому делиться полезными знаниями друг с другом надо без оглядки на возраст. Стройте свою цифровую крепость вместе!

Итак, коротко повторим основные темы книги.

«В однобортном уже никто не воюет»: обновляйте софт регулярно

Обновление в ИТ — это не бездумная гонка за модой. В новой версии софта, прежде всего, важны не форма и цвет кнопочек, а устранение пробелов в безопасности. Все операционные системы и программы, установленные на компьютере

и телефоне, потенциально уязвимы. Это только вопрос времени и желания хакеров — найти брешь и начать ее использовать.

Поэтому неукоснительно соблюдайте правила обновления:

- Не выключайте функцию автообновления в операционной системе, пусть все патчи и апдейты устанавливаются сами;
- Регулярно проверяйте, не пора ли обновить драйверы;
- Не сидите на старых версиях операционных систем. Windows 7 еще может работать, но защищать ее никто не будет;
- Всегда обновляйте ваш антивирус, VPN и другие средства защиты;
- Не мешайте обновлению браузера, если он хочет это сделать. Прервите работу и дайте ему перегрузиться;
- Обновляйте все прочие приложения, с которыми вы работаете.

Кто-то скажет: «А может, ну его»? Не зря же программисты шутят про обновленные версии: старые ошибки исправили, а новые внесли. И уязвимости все равно будут.

Возможно. Однако, про старые «дыры» хакеры уже знают, а про новые — еще нет. Поэтому все-таки лучше обновляться, чем этого не делать.

Всегда носите маску: помните про антивирус

С антивирусом все просто — он должен стоять и работать. Это средство по-прежнему эффективно против большинства известных угроз. Если вам вдруг «повезет» словить какой-то новый вирус, то защита может и не сработать, но это не повод ею пренебрегать. Точно также ношение медицинской маски не гарантирует абсолютной защиты от вируса, но значительно снижает вероятность заразиться.

> *Никогда не выключайте антивирус. Не обращайте внимания на тех, кто считает, что он тормозит работу и зря расходует ресурсы компьютера.*

И уж тем более не делайте этого, если вас попросит какая-нибудь программа, скачанная из Сети: «Ах, ваш антивирус мешает мне установиться!»

Ключи ко всем дверям: наведите порядок в паролях

Беззаботные времена, когда ключ от входной двери прятали под ковриком или в цветочном горшке, увы, прошли. Сегодня мы устанавливаем стальные двери с хитрыми замками, чтобы обезопасить свое жилище. Точно также следует поступить и с вашим цифровым хозяйством: наведите порядок в своих паролях и поддерживайте его.

- В первую очередь, позаботьтесь о паролях к самым важным сервисам — электронной почте, на которую регистри-

руете свои аккаунты, социальным сетям (потому что это доступ к вашей репутации и друзьям), облачным хранилищам, где лежат ваши фотографии и документы. Используйте для них уникальные и сложные пароли, но такие, какие вы сможете запомнить, ибо они могут вам понадобиться в любой момент.

- Включите везде двухфакторную аутентификацию. Лучше лишний раз ввести проверочный код, чем дать шанс злоумышленникам похитить ваши данные.

- Разберитесь с менеджерами паролей, выберете себе один из них и настройте. Потому что запомнить все нереально, все равно вам придется вести какие-то записи, — уж лучше это делать с помощью специального инструмента, чем держать файл с паролями на видном месте.

- Возьмите за правило сразу менять пароли на всех умных устройствах, как только они попадают в ваш дом — wi-fi-роутеры, компьютеры, телефоны, smart TV, пылесосы, кофеварки, холодильники и так далее. Неважно, новые они или б/у.

- Если есть основания считать, что пароли «утекли», меняйте их немедленно. Например, если вы потеряли телефон или ноутбук, срочно найдите какое-нибудь устройство и поменяйте все важные пароли.

Проследите, чтобы эти правила выполнял весь гарнизон вашей цифровой крепости, включая старых и малых. Если им трудно справиться с чем-то самим, настройте все так, чтобы им было удобно, но не ослабляя при этом безопасность. На-

пример, тот же менеджер паролей избавит их от необходимости ввода сложной последовательности букв и цифр.

Подстелить соломку: облака и резервное копирование

Может случиться так, что, несмотря на все принятые меры защиты, киберпреступники все-таки прорвут вашу оборону. Наиболее реальная угроза сегодня исходит от вирусов-шифровальщиков, поэтому лучше подстраховаться заранее, чтобы не зависеть потом от милости хакеров, которые, даже получив выкуп, могут не дать вам ключ расшифровки.

Для этого настройте резервное копирование (бэкап) всех ценных данных.

> *Проще всего делать бэкап в облако[1] — тогда процедура будет выполняться автоматически хоть каждые 5 минут, и вы почти ничего не потеряете в случае атаки. Если же вы готовы положиться на собственную дисциплину, то можно делать бэкап на внешний жесткий диск.*

Кроме того, резервное копирование убережет ваши данные в случае поломки или утраты компьютера.

Не забудьте и про данные с телефонов — контакты, заметки и особенно фотографии, — все это можно автоматически копировать в облако (или даже в два — для большей надежности).

---

1 Например, с помощью Acronis Ransomware Protection (есть бесплатная версия).

Друзья в соцсетях: никогда не разговаривайте с неизвестными

Надежнее считать, что пока не доказано обратное, все в интернете — неизвестные. Понятно, что не будет большой беды, если вы поговорите с незнакомым человеком о природе и погоде, но ни в коем случае не откровенничайте с ним (или с ней) о личных делах. И уж совершенно точно не перечисляйте сразу никому и никуда никаких денег, даже если просит знакомый. Сначала убедитесь, что его аккаунт не захватили хакеры.

Не перечисляйте сразу никому и никуда никаких денег, даже если просит знакомый.

Как это сделать? Самое простое средство — видеозвонок. Но когда друг новый, то даже такая проверка не гарантирует, что он вам не врет. И если нет возможности проверить информацию о человеке, лучше держаться от него подальше.

Будьте трижды осторожны, получив предложение встретиться в реале, или, как говорят, «развиртуализироваться».

И самое главное: будьте трижды осторожны, получив предложение встретиться в реале, или, как часто говорят, «развиртуализироваться». С одной стороны, мы живем в мире, где онлайн-знакомства стали нормой — люди встречаются, влюбляются, а сейчас уже и женятся в интернете. С другой — маньяки, грабители, шантажисты и другие преступники тоже умеют пользоваться соцсетями и мессенджерами.

Фишинг: а что скажет нам интуиция?

Уж сколько раз твердили миру, что не надо открывать подозрительные письма и кликать на подозрительные ссылки!

> *Кибержулики только того и ждут, чтобы запустить вам вируса-троянца, подсунуть фальшивый сайт вместо настоящего интернет-магазина или банка.*

Как отличить подозрительную ссылку от неподозрительной? Вообще-то говоря, никак. Надо честно признать, что абсолютно надежного способа распознать фишинг не существует. Развивайте интуицию и включите все уровни защиты, о которых мы говорили.

Как это развидеть? Встреча с нежелательным контентом

К сожалению, в интернете полно не только самой разнообразной полезной информации, но и всяческой грязи. Естественно, взрослые хотят оградить детей от встречи с недетским контентом: на уровне страны этим занимается Роскомнадзор, а дома вы можете использовать средства родительского контроля.

Но надо отдавать себе отчет в том, что все технические меры по фильтрации контента эффективны лишь отчасти.

> *Рано или поздно ваш ребенок все равно увидит то, что вы предпочли бы от него спрятать. И тогда от вас потребуется адекватная реакция, открытость и готовность к разговору*

на любые темы. Избежать этого не удастся: наказания и угрозы только разожгут интерес к запретным плодам, а игнорирование проблемы и попустительство может привести к психической травме.

Как быть? Готовьтесь заранее. Подумайте над тем, что и как сказать ребенку. Посоветуйтесь с психологом. Самое главное, что от вас требуется, — выстроить доверительные отношения. Но эта тема уже выходит за рамки нашей книги.

Каждый шаг оставляет след, цифровой

Поэтому все, сказанное вами, может быть использовано против вас. Прежде всего, это касается соблюдения закона: реальность такова, что неразумный пост, комментарий и даже просто неосторожный лайк могут иметь юридические последствия. Например, если размещенный подростком клип модной группы признан экстремистским, то сам подросток становится распространителем экстремистской информации.

Законодательство РФ в части регулирования интернета чрезвычайно динамично и непредсказуемо, поэтому трудно дать исчерпывающие рекомендации на тему того, что можно и чего нельзя делать в Сети. Как минимум, нелишним будет напомнить, что анонимность в интернете весьма условна, — обычному пользователю не под силу запутать следы настолько, чтобы его не нашли.

Поэтому стоит донести до ребенка простую мысль: интернет — это публичное пространство, и вести себя в нем нужно точно также, как в любом другом общественном месте.

От автора

Современную жизнь невозможно представить без интернета. И чем дальше, тем все более «цифровым» будет становиться наш образ жизни. Невзирая на все опасности и угрозы, мы будем каждый день выходить в Сеть, чтобы узнавать новости, делать покупки, общаться с друзьями, работать, учиться, развлекаться — другого варианта попросту нет.

Поэтому всем нам придется усвоить правила кибергигиены и обучить им своих детей. Это настолько же жизненно важно, как привычка мыть руки, приходя с улицы. При этом правила должны быть понятны, иначе они превратятся в пустые ритуалы, которые можно заставить выполнять только из-под палки.

Цель этой книги заключается как раз в том, чтобы объяснить, почему ради вашей безопасности в интернете надо поступать именно так, а не иначе. Это знание поможет вам наполнить смыслом те простые, в общем-то, правила кибергигиены, о которых сегодня столько говорится, и позволит относиться к своей кибербезопасности более осознанно.