3. Не держите Bluetooth постоянно включенным, включайте его только в случае необходимости (а если уж приходится держать Bluetooth постоянно включенным, используйте режим «Скрытый»).

4. Если вам пересылают по Bluetooth какой-то подозрительный файл, вы всегда можете отклонить его прием.

Как удалить зараженные файлы

Как правило, непосредственно с мобильного телефона (обычного, не «смарта») удалить зараженные файлы не удается. Для удаления зараженных файлов нужно подключить телефон к ПК и воспользоваться каким-либо файловым менеджером, например, для телефонов Nokia - диспетчером файлов, входящим в состав Nokia PC Suite. После удаления зараженных файлов перезагрузите мобильник (выключите и снова включите). Если удаление зараженных файлов не помогает, придется «перепрошить» телефон, обратившись в сервисный центр.

Предупрежден - значит вооружен

Мобильные вирусы существуют! Это уже не миф, а реальная угроза. До недавнего времени считалось, что вирусы если и угрожают, то только продвинуто-навороченным мобильникам, владельцам обычных мобильников бояться нечего. Увы, это уже не соответствует действительности! Доля обычных телефонов как минимум на порядок превосходит долю смартфонов.

Первоначально существовавшая грань между мобильными и компьютерными вирусами стерта. Теперь эти устройства могут взаимно заражать друг друга, причем компьютерным вирусам для широкого распространения потребовалось более двадцати лет. Мобильные вирусы прошли этот путь всего лишь за два года (очевидно, что мобильные «вирусописатели» активно используют опыт создания и распространения компьютерных вирусов).

В мире насчитывается около 3 млрд абонентов сотовой связи. Многие буквально не расстаются со своими телефонами, хранят в них конфиденциальную информацию. Нетрудно представить масштабы последствий в случае возникновения эпидемий мобильных вирусов.

Ольга ЛУСТЕНКОВА.

Мобильные телефоны изменили мир - нет нужды это доказывать. Факты, описанные ниже, лишь показывают, как сильно он изменился.

6 НЕИЗВЕСТНЫХ ФАКТОВ О МОБИЛАХ

1 ИХ МНОГО

Во всем мире насчитывается около 3,3 миллиарда благополучно функционирующих мобильных телефонов. Вдумайтесь в эту цифру - звонящих устройств всего-то в два раза меньше, чем населения земного шара. Если учесть, что мобильными телефонами пользуется не все человечество, а только взрослая и наиболее активная его часть, то на 100 человек приходится 158 работающих мобильников. Перебор?

2 ПЛАНЕТА В ОПАСНОСТИ

125 млн.мобильных телефонов в год отправляются прямиком в мусорное ведро. Нет, они не выходят из строя, а лишь надоедают своим владельцам, которые не прочь сменить былого любимца на что-нибудь новенькое и модное (корейцы, например, меняют мобильники каждые 11 месяцев). Очевидно, что человечеству скоро придется столкнуться с проблемой утилизации. Окружающая среда загрязняется в масштабах, которые трудно вообразить: только подумайте, какой у обычного телефона период полураспада...

3 ОНИ СКОРО ЗАМЕНЯТ БЮЛЛЕТЕНИ

Крошечная Эстония неожиданно для мирового сообщества стала лидером в области внедрения передовых технологий в процесс осуществления конституционного права на выбор. Проще говоря, теперь любой избиратель может отдать голос за понравившегося ему кандидата с помощью мобильного телефона. Это, с одной стороны, облегчает процесс голосования, а с другой - процесс идентификации личности избирателя. Эру «мобильного голосования» можно официально считать открытой.

4 КОРЕЙЦЫ «ПОДСЕЛИ» НА СМС

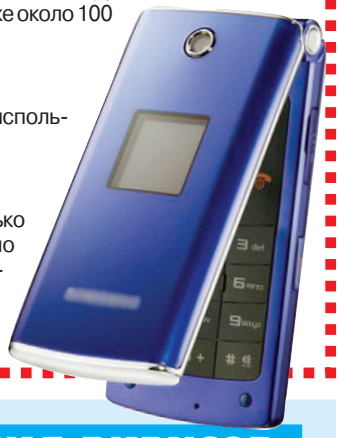
По статистике, корейский подросток посылает со своего мобильного телефона около 20 000 текстовых сообщений в год (около 60 смс в день). Согласно другим данным, около 30% корейских студентов отправляют уже около 100 сообщений в день. Когда они успевают учиться?

5 ПОЧТИ ФОНАРИК

Больше половины владельцев сотовых телефонов используют подсветку аппарата в качестве фонарика.

6 ОРУДИЕ ХУЛИГАНА

С помощью мобильного телефона можно хорошенько напугать его владельца. По крайне мере, в Англии неуклонно растет число угроз, посланных с помощью текстовых сообщений. СМС-угрозы «хороши» тем, что запугивать жертву можно круглые сутки: мобильный телефон у большинства людей включен всегда.



ЗАПОМНИ ИХ ИМЕНА

ЭНЦИКЛОПЕДИЯ ВИРУСОВ
(список далеко не полный)

Cabir. Вирус создан для размножения на аппаратах под управлением операционной системы Symbian OS. Появился в 2004 году. Распространяется только посредством Bluetooth-соединения. После попадания на смартфон начинает постоянно сканировать эфир с целью поиска новых жертв. Помимо банального самовоспроизведения, никакой опасности для смартфонов Cabir не несет, кроме разве что увеличения быстроты разряда батареи вследствие активного использования технологии Bluetooth.

CommWarrior. Предположительно разработан российскими хакерами, так как в своем коде имеет фразу «Отморозкам нет!». При заражении предлагает инсталлировать себя, заведомо маскируясь под какую-нибудь программу: утилиту-менеджера виртуального рабочего стола, программу для просмотра порнокартинок, антивирус. Распространяется по Bluetooth или MMS.

Duts. Является первенцем среди вирусов для смартфонов. Вирус в виде файла размером 1520 байт может попасть в аппарат по любым каналам связи с внешним миром. После проникновения в систему Duts выводит на экран следующий текст: «Dear User, am I allowed to spread?» (Дорогой пользователь, вы позволите мне размножиться?). Те, у кого хватит ума ответить на этот запрос «да», установят вирус на свой мобильный телефон.

Lasco. Типичный червь, поражающий сотовые телефоны. Распространяется двумя способами: посредством уже опробованной для этих целей Bluetooth-связи и через исполняемые файлы. Второй способ в мобильных телефонах встречается впервые. В его рамках происходит инфицирование установленных на телефоне SIS-файлов, добавление в их конец строчки velasco.sis (размер порядка 12 кбайт) и модификация заголовков. Установка зараженного SIS-приложения приведет к его автоматическому запуску. Однако, как и прежде, у пользователя будет запрошено подтверждение на установку вируса.

Mabir. По сути это просто слегка доработанная версия червя Cabir, которая, в отличие от него, может распространяться еще и в MMS-сообщениях. Новая функция реализована интересным образом: червь рассылает себя не по всем номерам из телефонной книги, а только в ответ на входящее SMS- или MMS-сообщение, причем ответное послание не содержит ничего, кроме вредоносного файла info.sis.

Dampig. Первое упоминание о нем датируется январем 2005 года. Распространяется в виде файла с расширением SIS, маскируясь под «крэк»-приложения FSCaller (программное обеспечение компании Symbian, из чего можно сделать вывод о списке потенциальных жертв).