

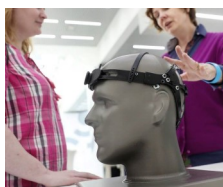


24.04.2019

НОВОСТИ IT-ТЕХНОЛОГИЙ

ДАЙДЖЕСТ № 55

В РОССИИ НАЧАЛОСЬ ПРОИЗВОДСТВО ГАРНИТУРЫ, ПОЗВОЛЯЮЩЕЙ ОБЩАТЬСЯ СИЛОЙ МЫСЛИ



Устройство "Нейрочат", позволяющее общаться силой мысли, запущено в серийное производство. Оно создано российскими разработчиками. Первая партия составит несколько сотен аппаратов. Устройство позволит набирать на компьютере тексты усилием мысли. Стоимость аппарата составляет 120 тысяч рублей. Возможно, пациенты с серьезными нарушениями речи смогут получить за него компенсацию из бюджета.

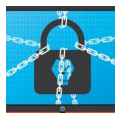
Источник: <https://life.ru>

КАКИЕ ПАРОЛИ НЕ ЗАЩИТЯТ ОТ ХАКЕРОВ ПОЧТУ И КОШЕЛЕК

Несмотря на растущее число хакерских атак, пользователи интернета никак не научатся уделять должное внимание подбору надежных паролей. В рамках исследования были выделены пароли, наиболее часто применяемые пользователями. В десятку самых популярных паролей вошли: 123456, 123456789, qwerty, password, 12345, qwerty123, 1q2w3e, 12345678, 111111, 1234567890. Самыми популярными кириллическими паролями стали: я (единственный односимвольный пароль), пароль, йцукен (qwerty только на кириллице), а также персонально-сентиментальные любовь, привет, люблю, наташа, максим, андрей, солнышко.

Источник: <http://35media.ru>

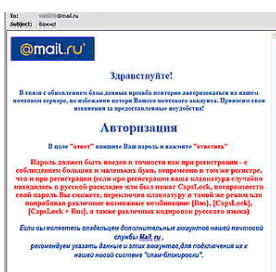
GOOGLE И «ОДНОКЛАССНИКИ» ЗАПУСТИЛИ ТЕСТ НА ТЕМУ БЕЗОПАСНОСТИ В ИНТЕРНЕТЕ



Благодаря проекту пользователи смогут узнать о том, как не попасться на уловки мошенников. Соцсеть «Одноклассники» совместно с Google запустила игровой тест на знание правил безопасности в интернете. С его помощью пользователи смогут узнать об основных правилах безопасного серфинга в сети и проведения времени в соцсетях. Опрос по заказу Google показал, что 30% пользователей хоть раз сталкивались со взломом аккаунтов в соцсетях, а 43% получали фишинговые сообщения.

Источник: <https://megaobzor.com><https://vk.com/maudomuk>https://www.instagram.com/maudomuk_kirishi

НЕМНОГО КОМПЬЮТЕРНОЙ ГРАМОТНОСТИ



Фишинг (англ. *phishing* от *fishing* «рыбная ловля, выуживание») — вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям. Это достигается путём проведения массовых рассылок электронных писем от имени популярных брендов, а также личных сообщений внутри различных сервисов, например, от имени банков или внутри социальных сетей. В письме часто содержится прямая ссылка на сайт, внешне неотличимый от настоящего, либо на сайт с редиректом.

Источник: <https://ru.wikipedia.org>