В ЦЕНТРЕ ВНИМАНИЯ

Что нового?

Как изменилась жизнь с 1 января 2018 года

МРОТ

В конце года был принят закон о повышении минимальной зарплаты (МРОТ) до уровня прожиточного минимума. До 1 января МРОТ в Тверской области составлял 7800 рублей, с 1 января 2018 года он установлен на уровне 9489 рублей в месяц, а с 2019 года — всегда будет равен прожиточному минимуму за второй квартал предшествующего года. Меньшие выплаты будут являться грубым нарушением трудового законодательства и могут привести к административной или уголовной ответственности. От МРОТ зависит размер различных пособий — больничных, детских, декретных.

ПЕНСИИ

С 1 января пенсии проиндексируют на уровень инфляции — 3,7%. Правда, повышение коснется не всех, а только неработающих пенсионеров.

ВЫПЛАТЫ ПРИ РОЖДЕНИИ ПЕРВЕНЦА

С нового года российские семьи начнут получать ежемесячные выплаты за рождение первого ребенка. Право на получение этих выплат будет у семей, чей доход меньше 1,5-кратной величины прожиточного минимума трудоспособного населения в регионе (в Тверской области он сейчас составляет 11050,61 рубля, пересчитывается раз в квартал). Деньги будут выплачивать, пока ребенку не исполнится 1,5 года.

МЕССЕНДЖЕРЫ

В России введен запрет на анонимное использование мобильных мессенджеров. Услуги по передаче мгновенных сообщений теперь будут предоставляться только пользователям, идентифицированным на основании абонентского номера и соответствующего договора. Для заключения такого договора потребуются паспортные данные.

ЖКХ

С 1 января 2018 года УК, ТСЖ и ЖСК начнут штрафовать, если те не будут размещать информацию в ГИС ЖКХ — это портал dom.gosuslugi.ru, где можно будет проверять работу управляющих компаний онлайн: смотреть финансовые отчеты, информацию о привлечении к административной ответственности, узнавать контакты диспетчерской службы и другие сведения.

ДЕТСКАЯ БЕЗОПАСНОСТЬ

В этом году наконец вступит в силу долго откладывавшийся запрет на перевозку групп детей автобусами старше 10 лет. Обязательным будет наличие тахографа и навигационной системы ГЛОНАСС или ГЛОНАСС/GPS.

Правда, Правительство РФ отложило введение запрета на полгода — до 1 июля 2018 года.

БАНКРОТСТВО

Вступили в силу поправки к закону «О несостоятельности (банкротстве)». Физическим лицам, которые не могут исполнять обязательства перед кредиторами, будет проще объявить себя банкротом — госпошлина снижена с 6000 рублей до 300 рублей.

АВТОМОБИЛИ

Самые большие изменения затронули владельцев транспортных средств. Акцизы на топливо с 1 января повышаются на 50 копеек за литр, эксперты прогнозируют рост розничных цен на 60 копеек.

Выросли штрафы за тонировку (1500 рублей в первый раз и 5000 рублей за повторное нарушение). Судебные приставы получили право отбирать водительское удостоверение за долги свыше 10000 рублей.

С 1 января 2018 года автомобилистов можно будет штрафовать по видеозаписям, полученным от третьих лиц.

Увеличивается «период охлаждения» при заключении договора ОСАГО — чтобы отказаться от ненужных услуг, у автовладельца теперь будет не 5 рабочих, а 14 календарных дней. Сами полисы ОСАГО поменяются — на них будут наносить QR-код с подробной информацией о договоре.

В 2018 году на некоторых территориях, где скорость ограничена до 10-20 км/ч, можно будет увидеть новые знаки «Зона успокоенного движения» — там нужно будет уступать пешеходам в любом месте, где они решат перейти дорогу. Обгоны на таких участках теперь запрещены.

БЕЗОПАСНОСТЬ

Ловцы цифровых денег

В России за последнюю пятилетку число киберпреступлений выросло в 6 раз

Киберпреступность стала хорошо организованным и очень прибыльным бизнесом. По разным оценкам, глобальный ущерб от нее по итогам 2017 года составит до 1,4% мирового ВВП. При этом раскрываемость таких преступлений крайне невелика.

О правилах, соблюдение которых поможет вам не стать жертвой «цифровых» воров, мы беседуем с заместителем управляющего Отделением Тверь ГУ Банка России по Центральному федеральному округу Вадимом Тетиным.

— Вадим Вадимович, вы можете рассказать о способах, какими кибермошенники залезают в наши виртуальные кошельки?

— Вы или ваши знакомые наверняка получали СМС с сообщением о блокировке карты, которое потом оказывалось фальшивкой. Самое удивительное то, что о такой схеме обмана знают практически все, но многие до сих пор попадаются на эту удочку. Получив такое сообщение, не паникуйте и ни в коем случае не связывайтесь с его отправителем по телефону, номер которого указан в СМСке. Сразу позвоните в свой банк (номер есть на вашей карте). И вам наверняка подтвердят, что с картой все в порядке. И, разумеется, сообщите о попытке мошенничества.

Еще один из распространенных видов мошенничества с картами — письма с вредоносными файлами. Они приходят обычно по электронной почте или через мессенджеры, часто маскируются под «выгодные предложения» или прайс-листы. В таком письме может быть вложение либо ссылка, кликнув на которую, вы запускаете компьютерный вирус. Вредоносная программа («зловред») похищает логин и пароль онлайн-банка и отправляет их злоумышленнику. Еще хуже, если такую ссылку вы открываете с мобильного устройства, — тогда мошенники узнают и код подтверждения операции из СМС-сообщения, которое присылает банк. Тогда вы наверняка можете проститься с вашими деньгами.

Год назад компания «Яндекс» сообщила, что конфиденциальные данные о банковских картах пользователей воруются посредством расширений для браузеров. Киберпреступники научились похищать данные, распространяя вредоносные плагины с более 80 тыс. сайтов в интернете. Это зараженные программные расширения, снабжающие пользователей полезной информацией без захода на специальные сайты — курсы валют или прогноз погоды. Такие программы распространяются через магазин расширений или из непроверенных источников, они могут исполняться как в стационарных, так и в мобильных версиях браузеров. Устанавливая эти плагины, пользователь открывает злоумышленникам доступ к паролям, логинам и данным банковских карт. Ежемесячно с такими проблемами сталкиваются более 1,2 млн пользователей.

— То есть сегодня, если вы пользуетесь онлайн-банкингом, нужно заботиться не только о том, чтобы не потерять смартфон, но и всеми возможными способами защитить находящуюся в нем личную информацию?

— Совершенно верно. В последнее время наибольший рост числа атак фиксируется именно в сегменте мобильных платформ. А Россия оказалась лидером по количеству мобильных банковских троянов, то есть программ, предназначенных для кражи финансовой информации пользователей. В отчете компании «Лаборатории Касперского» говорится, что в прошлом году количество вредоносных установочных программ на мобильных устройствах по всему миру выросло по сравнению с 2015 годом в три раза — до 8,5 млн. При использовании для проведения операций компьютера и мобильного телефона (все-таки это два независимых канала) информационная безопасность в известной степени обеспечивается. Если же вы совместите в одном месте и программу, и аутентификацию, и подтверждение платежа — этот порог заметно снижается.

— Значит ли это, что самоуверенность современного пользователя часто играет на руку кибермошенникам?

— Именно так. Раньше мы говорили о том, что наиболее поддающиеся на уловки кибермошенников — это люди пенсионного возраста, вели с ними большую разъяснительную работу, повышали их финансовую грамотность. А сейчас в лапы к мошенникам все больше попадают люди в возрасте до 40 лет: они очень активно пользуются гаджетами и технологиями, не сильно задумываясь о правилах. По мнению экспертов, основными проблемами на протяжении последних четырех-пяти лет остаются: опасность заражения мобильного устройства и компьютера через интернет, недостаточность встроенных средств защиты в программные продукты со стороны разработчиков систем дистанционного банковского обслуживания, а также невыполнение пользователями элементарных требований безопасности.

Ключевой проблемой следует считать именно уязвимость клиента. Какое бы средство защиты ему ни предоставлялось, оно может быть скомпрометировано – в том числе и самим пользователем. Чаще всего злоумышленникам удается обойти самые совершенные средства защиты по причине доверчивости клиента, его неосведомленности, халатности в отношении персональных данных. Именно поэтому злоумышленники все чаще используют не технические, а психологические приемы — то, что называется «социальной инженерией».

Чаще всего социальные инженеры воздействуют на желание быстро разбогатеть, получить что-то «на халяву», стремление купить что-то с большой скидкой. Очень часто давят на родственные чувства, страх за близкого человека: например, сообщают, что близкий человек якобы попал в беду. Особенно подвержены такому воздействию пожилые люди, которые, услышав о беде с дочкой, внучкой или Жучкой, сразу бегут к банкомату и делают то, что им говорят злоумышленники.

— Вот мы и подошли к вопросу финансовой грамотности, о которой так много разговоров последнее время.

— Не только разговоров, но и дел. Теме кибербезопасности в рамках программы повышения финансовой грамотности населения уделяется большое внимание. Например, в нашем регионе в ноябре прошли Дни малого и среднего бизнеса, в которых приняли участие сотрудники Отделения Тверь. Первыми мероприятиями в их рамках стали обучающие семинары для тверских предпринимателей по теме защиты от кибермошенников.

Завершая наш сегодняшний разговор, хочу дать несколько советов, следуя которым, можно в существенной степени обезопасить себя от киберкражи персональных данных и средств. Ни в коем случае не реагируйте на звонки и электронные сообщения, в которых вас просят предоставить реквизиты счета, PIN-коды, пароли или персональные данные. Всегда используйте надежные уникальные пароли для максимально возможного количества учетных записей в интернете, а лучше всего — индивидуальный пароль для каждой из них. Не храните логин и пароль на своем смартфоне: в электронном сообщении, в виде заметки или для «автоматического заполнения» при открытии интернет-сайта или приложения. Не ленитесь проверять выписки по банковским счетам и картам на предмет подозрительных транзакций.