

NEWS BLAST



High-Net-Worth Worries

Personal Umbrella Essential to Protect Your Assets



FOR HIGH-NET worth individuals, the financial consequences of being sued can be serious business.

They typically have more assets at risk should they be hit with a large court settlement or judgment and, while compensatory damages may be standard across the board, some juries have seen fit to punish the rich especially hard for their negligence.

But if you don't think it can happen to you, consider these scenarios:

- You host a charity function at your home and when 65 guests are on your deck, it collapses, injuring many.
- One of your children is involved in cyber-bullying a child and his parents sue your child for inflicting emotional harm.
- You are at fault in an auto accident that kills two passengers in the other car and severely injures the driver.

While your underlying automobile or homeowner's policy would pay for many of these damages, the policies usually cap liability payouts at a certain amount – typically \$500,000.

Any damages above that would come out of your pocket, unless you have an umbrella policy, which will kick in after your primary insurance limits are breached.

But the problem for high-net-worth individuals is that a typical umbrella policy is often capped at \$5 million, and that may not be enough if a large judgment is leveled against you.

Your assets could be at risk in the event of an especially large judgment.

Fortunately, there is a select group of companies that offer specialized personal umbrella policies that have limits as high as \$100 million – and they can be customized specifically to your situation.

Why you need it

As a high-net-worth individual, you also have more liability risks than most individuals, since you are more apt to:

- Hold a charity function or other event at home
- Serve on boards of directors
- Have swimming pools, trampolines and personal watercraft
- Employ residential staff like maids, nannies, drivers and gardeners.

How the policy works

The policy sits on top of the liability portion of your automobile or homeowner's policy and begins to pay when you've exhausted the limits of the primary policy.

There are two main types of liability that the policy will cover:

- Physical injury to someone and personal injuries (such those sustained from slander or defamation).
- Property damage to a third party that was caused by the insured. ❖



CONTACT US >>>

PLACER
INSURANCE AGENCY

If you have any questions regarding any of these articles or have a coverage question, please call us at:

Placer Insurance Agency

5 Sierra Gate Plaza, Second Floor
Roseville, California 95678
Phone: (916) 784-1008
Toll Free: (800) 642-5037
E-mail: newsletter@placerins.com

License No.: 0C66701

Online Security

A Hacker's Tips on Keeping Your Personal Data Safe

ONE BIG concern for all of us these days is online safety and protecting our personally identifiable information and credit card information.

Not only that, but clicking on a nefarious link on a website or in an e-mail can unleash a cyber attack on your computer with bots rifling through all of your files.

In addition to online scams, criminals are also calling people and asking for personal information.

Recently, an anonymous hacker who now writes a cyber security blog had these recommendations for individuals who want to protect themselves and their files when online.

Here's the techie's advice:

- Check senders carefully. Cyber criminals will try to get you to click on a link in an e-mail by making it seem like it comes from an official source, like "auditor@irs.gov." If in doubt, don't click on any links and call the agency using information from 411 or other legitimate sources.
- Don't believe every caller. If you get a call from someone claiming to be from the IRS who tells you that you owe back taxes and face penalties that could involve asset forfeiture, you should know that the IRS doesn't make phone calls. Tell the caller that you'll call them back. Look up the number from scratch and call. More often than not, nobody will answer or the agency will never have heard of you.
- Don't follow links to a site that's going to ask for secure information, such as a password. "If I want to raid your bank account, or do other harm, one way I can do it is to send you an official-looking e-mail with a link to your bank, asking you to log into your account for some reason," the hacker writes. If you go to the criminal's site, they will then obtain your log-in information and have access to your bank account.
- Before you follow a link, verify that the visual link and the actual link match. For instance, let's say the link is "PETA.org." But if you move your cursor over the link without clicking, most browsers will then show you the real link, either near the cursor, or at the lower-left corner of the window. If you see something like "PETA.smurfit.org" or "PETA.ru," or anything else that doesn't exactly match, it's likely they're trying to dupe you.
- Don't automatically grant access for all programs. If you download a new game online and it asks you to enter the system manager password, you may be right to be suspicious as a game would not need system-level access.
- If you are using a new site that requires a password, use a unique password, and one that can't be found in a dictionary. In other words, don't reuse a password from another site. This way, if the site is compromised and they get your unique password, they won't be able to access other online accounts of yours.
- When a system asks for security questions and answers, give ridiculous answers. For instance, if a site asks which high school you went to, don't use the name of your real school. A dedicated hacker can find out where you went to high school. Instead, you might want to write something like "cuddly panda" or "fuchsia."
- Ignore spam e-mail. You can often tell that e-mail is spam before opening it. Look at the "From" address. Do you know anybody named "Special Offer?" If the subject is odd, like "Donald Trump says he has a big brain, here's why," it's likely spam and should be avoided.
- Set your e-mail reader so that it does not load images automatically or follow links automatically. For instance, if a scammer includes an image, allowing it to load can send the image ID to another server that then gains access to your system. Before you allow the browser to load images, check that every image name is generic. ❖



Home Security

Should You Install Electronic Door Locks?

AS OUR LIVES get more high-tech, one feature of your home may one day go the way of the typewriter: your house key.

From fingerprint sensors to Bluetooth and Wi-Fi-enabled systems, keyless entry products are rapidly transforming the way Americans secure their homes.

These keyless systems may not be for everyone, particularly anyone that's not comfortable with technology.

However, if you are tech-savvy these keyless entry systems add another layer of home protection that's not available from a typical door. And you don't have to ever worry about losing your keys again.

Are these easy-access locks the right choice for you? If you're not comfortable with technology, they probably won't be. However, if you have no problem programming your DVR, universal remote and household thermostat, a keyless lock may be a good option.

Here are some of the technologies currently on the market:

Biometric fingerprint recognition – This is the latest and greatest keyless entry technology. Biometric locks recognize your fingerprint, allowing you to unlock your home with a swipe of your finger. This type of keyless lock requires you to program it with your fingerprint as well as those of the rest of your family or others you want to allow to access your home.

Keyless deadbolts – These are less expensive than the fingerprint entry system. They are very dependable and also offer keyed entry alongside the digital keypad for added peace of mind in case you forget your code.

Keyless remote door locks – These systems don't require keys or codes that you can forget. They include a fob similar to ones that you use for opening your vehicle. Using RFID technology, the door will open with the press of a button.

Smartphone-controlled locks – These locks synch with your mobile phone via Bluetooth. This allows you to control entry to your home remotely as well as track who is coming and going. Some of these locks will text you when someone else opens your home's door, while others will automatically unlock your door when you approach it.

Keypad locks – These entry systems require you to program an entry code. Though newer, more complex models may allow you to have individual codes for specific people or even program a greeting that will play when the door is unlocked.

Costs and security

Prices for electronic door locks range from \$100 to more than \$1,000, depending on the type of lock and features included. While they can make entering and exiting your home easier – unless there's a power outage or the circuit board fails – they aren't necessarily more secure than traditional keyed locks.

Burglars generally enter homes through unlocked doors or windows or by forcing open a window or door.

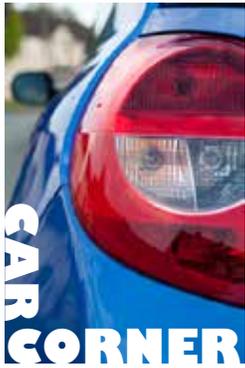
If security is your main concern, you're probably better off investing in solid wood or steel exterior doors rather than the latest electronic lock technology. Door jambs reinforced with steel plates will also make it more difficult for an intruder to kick in the door.

Whether you opt for traditional keys or a new, high-tech electronic lock for your home, you should make sure you are properly insured for a break-in. If you don't have homeowner's or renter's coverage, call us. ❖



Produced by Risk Media Solutions on behalf of Placer Insurance Agency. This newsletter is not intended to provide legal advice, but rather perspective on recent regulatory issues, trends and standards affecting insurance as well as instructional articles on protection and managing personal risk. Please consult your broker for further information on the topics covered herein. Copyright 2017. all rights reserved.

Car Seat Safety for Your Most Precious Cargo



ACCORDING TO the Centers for Disease Control and Prevention, motor vehicle injuries are the leading cause of death among children in the United States.

In 2015, 712 children aged 12 and younger died in auto crashes, and another 143,250 were injured.

Many of these deaths and injuries could have been prevented with the use of a proper child safety seat.

Car seat use reduces the risk of death for children under the age of 1 by 71%, and for kids aged 1 to 4 by 54%. Booster-seat use reduces the risk for serious injury in children aged 4 to 8 by 45% compared to the use of seat belts alone.

If you want to ensure children riding in your car are doing so safely, you'll need to do the following:

Know your state's child passenger safety laws

While requirements vary based on age, weight and height, all states require child safety seats for infants and certain children.

Many require children to ride in the rear seat whenever possible, as well as the use of rear-facing infant seats, forward-facing child safety seats, and booster seats for older children.

Make sure the seat is right for your child's size and age

Rear-facing car seats should be used from birth to the age of 1, at minimum. However, it's wise to keep your child in a rear-facing car seat

until they reach the age of 3 or outgrow the height and weight limits specified by the manufacturer.

At this point, you can transition your child to a forward-facing car seat until they are 7 or again outgrow the manufacturer's height and weight specifications.

Booster seats are recommended for children age 7 and older who cannot fit in a seat belt correctly without one.

Buy a seat recommended by the NHTSA

These seats meet federal safety standards as well as strict crash performance standards. You can find a list of the National Highway Traffic Safety Administration-rated car seats, along with information on their ease of use on the agency's website: www.nhtsa.gov.

Install and use the seat or booster seat properly

Install the seat according to the owner's manual instructions. If you need assistance, visit a car seat inspection station in your area.

Local law enforcement agencies may also hold periodic car seat inspection events.

Put your child in the middle of the back seat

When traveling with one child, or only one child in a safety seat, place them in the center of the back seat. In the event of a collision, this is the safest location in the vehicle.

Register your car seat with the NHTSA

If there is a recall, you will be informed by e-mail and you can act accordingly. ❖

