Hurricane season is here. Florida has 1,197 miles of coastline, and all of its cities are within 75 miles of the coast. There are no areas in Florida immune to the forces of a hurricane. If a hurricane strike becomes imminent, it will be imperative that you are prepared and informed both before and after the storm.

Have a Plan – Prior to the threat of a disaster, families can create a personalized Family Disaster Plan at FloridaDisaster.org/GetaPlan. This site provides checklists and important steps to take before, during, and after the disaster. The plan should also address the issue of pets. If you anticipate needing transportation or any specialized assistance, register now with your county emergency management agency.

Generator-Powered Gas Stations – Know which gas stations have been identified as having access to generator power during emergencies. The presence of generator power DOES NOT indicate that the station will be open for business or able to dispense fuel.

Price-Gouging – In the wake of a natural disaster, essential commodities may be in short supply. When an executive order is issued by the Governor declaring a state of emergency in Florida, you can call the Florida Attorney General’s Price Gouging Hotline at 866-966-7226 to report possible violations.
Home Repair – A frequent problem after a disaster is “fly-by-night” contractors who take deposits before starting work or final payments before finishing. If your home is in need of repair, check each contractor’s address, license, and complaint history by calling the Department of Business and Professional Regulation at (850) 487-1395 or by visiting their website at MyFloridaLicense.com. Be cautious of repair businesses or individuals who solicit door-to-door, arrive in unmarked vehicles, or claim they are from another area and are here solely to help disaster victims.

Food Safety – Keep in mind that food and water may be contaminated by floodwaters. Get safety tips at www.fdacs.gov/Divisions-Offices/Food-Safety.

Generator Safety – Never use a generator, grill, camp stove or other gasoline, propane, natural gas or charcoal-burning device inside a home, garage, basement, crawlspace or any partially enclosed area. Keep these devices outdoors, away from doors, windows, and vents that could allow carbon monoxide to come indoors.

Fuel – The potential for water contaminated fuel incidents increase after a considerable storm. If you witness flooding at a station during or immediately following a storm report it to the department so we can have an inspector check the storage tanks for water contamination. Always keep the receipt of purchase and report any possible contaminated fuel incidents to the department immediately.

Skimmers – Thieves will take advantage of power outages to install skimming devices. Always check for security measures on the pump and be aware of your surroundings. Look around for possible cameras, or any suspicious equipment that doesn’t belong on the pump. Please remember not all pumps require Security Tape. Some pump systems have internal security, ask the store personal about the pump security if in doubt. Report any evident signs of tampering or unauthorized access to fuel dispensers to the gas station manager and file a complaint with FDACS.

Insurance – Call your insurance agent to verify any messages or robocalls you receive about your insurance or insurance premiums after the storm.

Landlord/Tenant – If you live in a rental property that is damaged by a storm, you need to know your rights and responsibilities and those of your landlord. Visit Landlord/Tenant Law for more information or refer to Florida’s Landlord/Tenant Law, Chapter 83, Part II, Florida Statutes.
Do you wear contacts? If so, read on. You have the right to get your contact lens prescription from your eye care prescriber — whether you ask for it or not — at no extra charge. The Contact Lens Rule, which the Federal Trade Commission (FTC) enforces, says so. That lets you take your prescription wherever you want — online or to the mall — to shop around and look for the best deal.

Periodically, the FTC likes to take a look at its rules to make sure they are up to date, effective, and not overly burdensome. As part of a review of the Contact Lens Rule, the FTC looked at ways to make sure prescribers are giving patients a copy of the contact lens prescription once the contact lens fitting is completed. The FTC recently updated the Rule to help make that happen. The Rule changes go into effect 60 days after publication of the Federal Register notice.

Now, after giving you a copy of your prescription, prescribers have to ask you to sign a confirmation and keep it for at least three years. Prescribers can confirm that you got your prescription in one of four ways:

- ask you to sign a separate confirmation statement
- ask you to sign a copy of the prescription that has a confirmation statement, which the prescriber will keep
- ask you to sign a copy of the sales receipt for the examination that has a confirmation statement, which the prescriber will keep, or
- instead of a paper copy, the prescriber may give you a digital copy of the prescription, if you consent to the digital delivery and the method of digital delivery. The prescription must be accessible, downloadable, and printable. If the prescriber gives you your prescription electronically, she doesn’t have to ask you to sign a confirmation statement. She will, though, have to ask you to sign a consent form to get your prescription electronically. This is to make sure you know what you’re getting, and have the ability to use it.

If you suspect an eye care prescriber is violating the Contact Lens Rule, report it to the FTC at ftc.gov/complaint. For a more in-depth look at your prescription rights for contacts — and eyeglasses — take a look at Understanding Your Prescription Rights for Glasses and Contact Lenses. It includes a list of what you should see in your prescription.
In this age of social distancing, more and more of our favorite stores now offer ways to score great deals online. Even as shops around the country open their doors again, buying online is still a great, useful tool for people to enjoy. It’s nice to know that with a simple web search, you can find, buy, and ship almost any item right to your front door. But, while you’re enjoying that convenience, you want to be sure that sharing your financial and personal data online is safe.

Before you click “Place Order,” follow these tips on how to keep your data secure and save money as you shop:

- **Plan ahead by setting a budget.** Ask yourself how much you should spend and be sure to include delivery costs in your budget.

- **Determine what is most important to you about the item you are buying.** What are the must have features versus the ones that would just be nice to have?

- **Take a few minutes to compare products.** Type the product name into a search engine along with words like “review,” “complaint,” or “scam.” Read online reviews from other people who bought the item or from product experts. Look for feedback about how the product works and its overall quality.

- **Look for reviews about the company selling the product.** Read information about the company’s reputation and customer service. Don’t rely on just one source for information.

- **Verify the total cost of the product.** Check shopping comparison sites to compare the price of the product at different shopping sites. Remember shipping costs and other add-on costs may not be included in the listed price.

- **Look for online coupon codes.** Search the retailer’s name with terms like “coupons,” “discounts,” or “free shipping.”

- **Check out the terms of the deal.** Verify when you will receive your order. The law requires sellers to ship the item within 30 days of the sale. Can you get a refund if you must return the item, and who pays the shipping for returns? Is there a restocking fee?

- **Decide how to pay.** Credit cards give you some protections that other payment methods may not. If there is a problem, the law allows you to dispute charges and temporarily withhold payment while your dispute is investigated. Some companies cap your liability at $50 if someone uses your card without your authorization. Others may waive the charges entirely.

- **Verify the site is secure.** Before you enter your payment information, verify that the website address begins with “https.” The “s” stands for “secure” and means that your information is encrypted before it is transmitted.

If you have a problem with an online purchase or charge, try to work it out with the seller first. If you can’t resolve the problem, file a complaint at [www.FloridaConsumerHelp.com](http://www.FloridaConsumerHelp.com).
During these difficult economic times, scammers will do almost anything to try to get your money. Including, it turns out, making bogus claims about economic stimulus checks to lure customers to auto sales events.

In a complaint, the Federal Trade Commission says Traffic Jam Events, a direct mail marketing firm for car dealers, is falsely claiming in mailers that their “Economic Automotive Stimulus Relief Program” is affiliated with and approved by the government. It’s not.

They’re also claiming that people who come to designated sites will get stimulus relief checks. They won’t.

They’re even sending out checks that say “COVID-19 Auto Stimulus” with space to endorse the check on the back. But the checks are fake, there’s no car-related relief in the CARES Act, and the government isn’t using car dealerships to give out economic impact payments.

Here are three ways you can help protect yourself and others from these types of scams:

• When you get promotional mailers, check out the company before you act. Search online for the company name plus the words “scam,” “complaint,” or “review.”

• Don’t click on links in emails or text messages. If you click, you could download malware onto your device and wind up on a site that’s after your personal information. Instead, if you’re worried about the message, look up whoever sent it. Then call or email using a number your research gave you — not one from the message.

• Say NO to anyone who insists that you pay by gift card, wire transfer, or cryptocurrency. That’s how scammers tell you to pay, and no legitimate business will tell you to pay that way.
A recent Google Alert scam has caught the attention of many. Google Alerts recently caught fraudsters trying to push fake data breach notifications for big-name companies in an effort to distribute malware and damage people’s computer networks. According to Bleeping Computer, fraudsters have been mixing black-hat SEO, Google sites and spam pages to direct users to dangerous locations based on data breach information.

Google Alerts is designed to send notifications to people who sign up for specific keywords monitoring and provide search results. As part of this Google Alert scam, fraudsters were able to create pages and use compromising websites to combine “data breach” with well-known brands. Bleeping Computer reports that some of those well-known brands include Chegg, Canva, EA, Dropbox, Hulu, Shein, Ceridian, PayPal, Target, Hautelook, Mojang, InterContinental Hotel Group and Houzz.

In the Google Alerts, fraudsters offer giveaways and download offers, which lead to the dangerous malware. The threat actors are also believed to have used the Google Sites tool to build webpages to host their content. Bleeping Computer says they found that the scammers were pushing unwanted search-related extensions. As part of the Google Alert scam, malicious links were also believed to be sent to people with an iPhone 11 device for a fake giveaway. It claimed to be set up by Google as part of a “Membership Rewards Program” and the offer said the gift was “exclusively and only for Verizon Fios users.” Users had to fill out a survey, allowing scammers to get their money. Browser extension scams can pose a risk to browsing privacy because malware can be used as part of this method.

Consumers who use Google Alerts should be aware of this particular scam; going directly to the source (the purported breached entity) instead of clicking on an unknown link. The Identity Theft Resource Center (ITRC) has been tracking publicly-notified data breaches since 2005 and has the most comprehensive and the most readily available data breach information for publicly-notified breaches. Any consumer that wants to fact check the latest information regarding a publicly reported breach is encouraged to access ITRC resources to confirm any new circumstances. Consumers can sign up for the ITRC monthly data breach newsletter, as well as view monthly and yearly data breach reports. They can also receive a “risk score” on what their true concerns should be by visiting Breach Clarity and entering the particular breach on which they would like information.
COVID MASK EXEMPTION CARDS ARE NOT FROM THE GOVERNMENT

by Colleen Tressler, Consumer Education Specialist, FTC

To help limit the spread of the Coronavirus, many states are requiring people to wear face coverings in places open to the public. But there are cards circulating online and on social media that say the holder has a disability that prevents them from wearing a mask, and that it’s illegal for any business to ask them to disclose their condition. Variations of the card include the seal of the U.S. Department of Justice (DOJ), one of the federal agencies responsible for enforcing the Americans with Disabilities Act (ADA).

The fact is, these cards aren’t issued or endorsed by DOJ, or any other federal agency. DOJ urges the public not to rely on the information contained in these postings, and to visit ADA.gov for ADA information issued by the agency.

For information about your rights under the ADA, visit ADA.gov, or call 800-514-0301 or 800-514-0383 (TTY).