



# SWANSBORO COUNTRY PROPERTY OWNERS ASSOCIATION

Newsletter - November, 2019

Visit us at [SCPOA.info](http://SCPOA.info)

SCPOA.info and this newsletter are the only sources for official and accurate information about your association.

**Welcome to the November 2019 newsletter.**

---

**The SCPOA Board, and The Management Trust, wish all members and residents a wonderful Thanksgiving and a terrific Holiday Season.**

---

**Roadside** and airstrip vegetation spraying has been rescheduled for Thursday, November 21st.

---

**There** will not be an open SCPOA board meeting in December.

---

**The** board will convene on Saturday, November 23rd at 10 AM to review the 2020-2021 SCPOA Budget and hopefully finalize its approval as well.

---

**Self** nomination forms have been sent to all members of SCPOA. This is your opportunity to keep Swansboro a wonderful community. All members are encouraged to seek a position as a board member. For this election there will be 3 board positions available. Speaking of self nominations the board has selected Saturday, January 25, 2020, at 10 AM as the time for the candidates' meet and greet. This will be held at Dyer Lake Hall, 6770 Sluice St. Those seeking to become a candidate are strongly urged to attend this event. This will provide you the opportunity to provide members with your thoughts and ideas as to how to better Swansboro, prior to ballots being cast. Instructions to submit your form are contained at the bottom of that letter. We suggest that members await the candidate's meet and greet before casting your ballot. Ballots can be submitted at the annual members' meeting held on February 8, 2020 directly before the meeting begins at 10AM.

---

**The** maintenance department wants everyone to know there are literally mounds and mounds of wood chips available at the parking area of the maintenance building. They are free for the taking, so load up your trucks and help yourselves. Another way to obtain chips is to contact maintenance, 344-0498. Kevin has indicated he can provide a tractor full of wood chips. All chips are free. Most chips have mixed wood varieties but are all excellent mulch and ground cover.

---

**The** article on the next page deals with keeping yourself safe while online. This is being included as it seems as though the Holidays are 'prime pickins' for folks in regards to scams. Many ideas to safe guard your online presence are available and the enclosed lists are but a handful. Please be safe out there while surfing the web, or even your phone, and make it a Happy Holiday for all.

## Protect yourself! Here's some information to help you stay safer while online.

From identity theft and credit card fraud to phishing scams and malware, cybercrime today is real, rampant, and personal. Here are some tips to help you get cyber-savvy.

### **Strengthen Your Online ID and Password**

When a database containing usernames and passwords is stolen or hacked, criminals often try using that list of usernames and passwords on hundreds of other companies' websites to see if they can get into any other accounts. Don't use the same username and password combination on multiple sites, and avoid the most common passwords. For some fun reading, do an internet search for "most common passwords."

Use a password that is at least 8 characters long and contains an uppercase letter, a lowercase letter, a number, and a special character. As an example, pick eight characters (e.g., PB&J2eat), then add several characters from the site name that you are logging into. This way, you can still remember your password and it will be unique for each website.

In this example, we used "PB&J2eat", plus a simple description.

- www.mypowercompany.com PB&J2eatpower
- www.cellularphone.com PB&J2eatphone
- www.yourbank.com PB&J2eatbank

This way, if one of the companies got hacked, the other logins wouldn't be compromised.

When Personal Identification Numbers (PINs) are needed, don't use the most common PINs (like 1234) or all repeating numbers (1111, 7777, 5555, etc.). Banking industry studies have shown that the top 10 most commonly used PINs account for over 25% of PINs used. If a criminal tries the top 10 of the most frequently used PINs, they have over a 25% chance of gaining access.

### **Always Log Out of Your Account When You're Done**

Closing the browser window doesn't always log you out. If you walk away from your computer, someone else could re-open your browser and access your accounts. To protect yourself even further, learn how to delete your browser history and cookies for whatever browser you use. Browsers keep a history of what you do while you are online. If you use a public computer, you don't want to leave behind information about yourself that someone else could access.

### **Check Hyperlinks Before You Click**

Hyperlinks, which typically appear as blue underlined words, are normally used to take you to another website. However, they can take you somewhere other than that what link actually claims.

#### Check Hyperlinks

In Internet Explorer, Chrome, and Firefox, you can hover your mouse over a hyperlink to display the underlying link in the lower left corner of the browser window. On most mobile devices, you can press and hold a hyperlink to display the actual link destination. If the underlying link does not match where you are expecting to go, do not click on it.

### **Verify the Return Address Before Responding to Emails**

The return email address on an email can be spoofed (made to appear as if it came from a trusted person or company when it did not). The name that appears as the return address might not be where the email came from, and it might not be where a return email will go if you respond.

#### Verify the Return Address

Keep track of when you receive emails from a trusted source. Remember these trusted sources for future reference, and if need be by writing down the trusted email address(es). If you receive an email from a different email address, do not respond to it.

If you respond to a valid email from anyone, be aware that the information in the email is not protected. Unless you know for sure that your email is set up to be encrypted, don't send any personally-identifiable information in any email.