NATIONAL BULLETIN

February 2018

Congratulations! National residents have responded with overwhelming support to our yard debris policy. Please take a couple of minutes to review the current policy (Section IV. Paragraph B, "NPOA Rules & Regulations"). Your continued cooperation is appreciated by your neighbors.

B. Collection of Trash: Property owners will abide by the trash collection times and dates set by the contractor assigned to the City of Southern Pines. The manner of trash, debris and waste storage will be consistent with section 12.2.4 in the DC&Rs.

Trash containers and/or debris piles must not be kept at the curb an excessive amount of time as follows:

Household Trash: Trash containers or bulk trash of any kind are to be placed to the curb no earlier than Tuesday afternoon, the day prior to the Wednesday trash pickup day. All containers, or bulk trash not collected for any reason, must be removed no later than Thursday morning.

Yard Debris: If you use a service or individual for landscape maintenance, that service or individual must remove all yard debris from National or face fines and/or other penalties (yard maintenance policy details are available at the Security Gatehouse). Residents doing their own yardwork are encouraged to use a yard debris container. However, if it's necessary, or you wish to pile your yard debris, it must be placed at the curb, clearly within your property lines, no earlier than the weekend prior to the yard debris pickup day (the yard debris pickup schedule is available at the Security gatehouse). Note, yard debris container timing is the same as household trash.

Failure to properly adhere to the community's trash and debris policy will result in the following actions:

1st Offense: Written Warning
2nd Offense: Written Warning
3rd Offense: $100.00 fine
4th Offense and Thereafter: $250.00 fine for each occurrence

Notes:

a. *Residents are ultimately responsible for the payment of any fines levied against the landscape services or individuals they use.*
b. *If a resident has given permission to another to pile yard debris on their property, the resident giving that permission will be responsible for any fines or penalties levied for non-compliance to the above policy.*
c. *An occurrence is defined as any one violation that takes place between trash and yard debris pickup dates.*

Listed for your convenience are the YARD DEBRIS PICKUP DATES for 2018, which are every OTHER Wednesday; household trash is EVERY Wednesday).

January 10, 24	February 7, 21	March 7, 21
April 4, 18	May 2, 16, 30	June 13, 27
July 11, 25	August 8, 22	September 5, 19
October 3, 17, 31	November 14, 28	December 12, 27 (Holiday schedule)

It is the intent of the NPOA to preserve the beauty of the entire National Community and the preservation of your investment. Thank you for your understanding and cooperation with respect this matter.

Sincerely,
National Property Owners Association, Inc.

WASTE INDUSTRIES
welcome to a cleaner world!

1.866.423.4122
A www.wasteindustries.com

YOUR 2018 COLLECTION SCHEDULE

Thank you for being a Waste Industries customer! As we enter into 2018, we wanted to provide you with an annual waste & yard wast schedule for the new year. **The calendar below is marked with your area's collection dates.** You'll also notice that dates following a holiday will be picked up the following day.

We also would like you to know that safety for you, your family, and our employees remains our number one priority. During inclement weather, your schedule may be altered. You can track inclement weather alerts online at www.wasteindustries.com.

The following holidays may affect your service date:*

January 1st - New Years Day (2018)
November 22nd - Thanksgiving Day (2018)
December 25th - Christmas Day (2018)

*Collection services will be delayed by **ONE** day during the holiday week, beginning the date of the holiday.

You can also view collection schedules by accessing your account online at our website customer portal at wasteindustries.com/myaccount/login.

= Day of Trash Collection = Yard Waste Collection = Holiday

For pickup on or following a holiday, your collection will be delayed by one day.

January - 2018

S	M	T	W	T	F	S
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31			

February - 2018

S	M	T	W	T	F	S
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28			

March - 2018

S	M	T	W	T	F	S
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

April - 2018

S	M	T	W	T	F	S
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30					

May - 2018

S	M	T	W	T	F	S
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31		

June -2018

S	M	T	W	T	F	S
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30

July - 2018

S	M	T	W	T	F	S
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

August - 2018

S	M	T	W	T	F	S
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

September - 2018

S	M	T	W	T	F	S
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30						

October - 2018

S	M	T	W	T	F	S
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31			

November - 2018

S	M	T	W	T	F	S
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	

December - 2018

S	M	T	W	T	F	S
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31					

$1 MILLION
in donations to local charities with
The Full Circle Project

Your voice makes a difference. Select your charity class today by logging into My Account.
www.wasteindustries.com/myaccount/login

How to Beat Ransomware: Prevent, Don't React

Picture this: You've spent the last few weeks working on a tribute video for a friend's 30th wedding anniversary. You collected photos and video clips and edited them together, laying over a soundtrack of their favorite songs. It was a real labor of love.

When you finally finish the project, you go to copy the file onto a DVD and—what the?—a strange message pops up.

"The files on this computer have been encrypted. You have 96 hours to submit payment, otherwise your files will be permanently destroyed."

You've been hit with ransomware.

You didn't back up the anniversary video. In fact, you haven't backed up any of your files in months. What do you do?

Unfortunately, when it comes to ransomware, once your files are encrypted, there's not much you *can* do—besides cut your losses or pay up. And even if you do pay up, there's a chance you won't get your files back, so you're out the files and your cash.

For businesses around the world, the stakes are even higher. The recent outbreak of WanaCryt0r was the largest ransomware attack in the history of the Internet, freezing hospital workers out of critical data and disrupting operations of organizations in 150 countries.

These types of attacks can have a devastating impact, from losing precious personal data to shutting down hospital services in the middle of emergency procedures. In some cases, it's a matter of life or death.

That's why it's so important to prevent ransomware attacks from happening in the first place.

Types of ransomware

The first step in ransomware prevention is to recognize the different types of ransomware you can be hit with. Ransomware can range in seriousness from mildly off-putting to Cuban Missile Crisis severe.

Scareware
Okay, yes, it's called scareware, but in comparison to other types of ransomware—not so scary. Scareware includes rogue security software and tech support scams. You might receive a pop-up message claiming that a bajillion pieces of malware were discovered and the only way to get rid of them is to pay up. If you do nothing, you'll likely continue to be bombarded with pop-ups, but your files are essentially safe. A quick scan from your security software should be able to clear out these suckers. For simple instructions on how to clean an infected computer, check out the step-by-step guide below.

Pro tip: A legitimate cybersecurity software program would not solicit customers in this way. If you don't already have this company's software on your computer, then they would not be monitoring you for ransomware infection. If you do have this company's software, you wouldn't need to pay to have the infection removed—you've already paid for the software to do that very job.

Screen lockers
Upgrade to terror alert orange for these guys. When lock-screen ransomware gets on your computer, it means you're frozen out of your PC entirely. Upon starting up your computer, a full-size window will appear, often accompanied by an official-looking FBI or U.S. Department of Justice seal saying illegal activity has been detected on your computer and you must pay a fine.
In order to reclaim control of your PC, a full system restore might be in order. If that doesn't work, you can try running a scan from a bootable CD or USB drive.

Pro tip: The FBI would not freeze you out of your computer or demand payment for illegal activity. If they suspected you of piracy, child pornography, or other cybercrimes, they would go through the appropriate legal channels.

Encrypting ransomware
This is the truly nasty stuff. These are the guys who snatch up your files and encrypt them, demanding payment in order to decrypt and redeliver. The reason why this type of ransomware is so dangerous is because once cybercriminals get ahold of your files, no security software or system restore can return them to you. Unless you pay the ransom—they're gone. And even if you do pay up, there's no guarantee the cybercriminals will give you those files back.

Pro tip: The FBI has changed its position on whether folks should pay the ransom. They now agree with cybersecurity professionals, who advise you to avoid this option. Complying with ransomware criminals just opens the door up for future attacks. If, however, really valuable files are at stake, you can try to negotiate the release of the most important for less money. This should only be done as a last resort.

So what should you do to protect your files from this kind of ransomware? Get out in front of it.
"If any attack in the history of malware proves that you need protection in place before the attack happens, encrypting ransomware is it," says Adam Kujawa, Director of Malwarebytes Labs. "It's too late once you get infected. Game over."

Ransomware prevention
The first step in ransomware prevention is to invest in awesome cybersecurity—a program with real-time protection that's designed to thwart advanced malware attacks such as ransomware. You should also look out for for features that will both shield vulnerable programs from threats (an anti-exploit technology) as well as block ransomware from holding files hostage. Customers who were using Malwarebytes 3 Premium, for example, were protected from the WanaCrypt0r attack.

Next, as much as it may pain you, you need to create secure backups of your data on a regular basis. You can purchase USBs or an external hard drive where you can save new or updated files—just be sure to physically disconnect the devices from your computer after backing up, otherwise they can become infected with ransomware, too. Cloud storage is another option, but we recommend using a server with high-level encryption and multiple-factor authentication.

Then, be sure your systems and software are updated. The most recent ransomware outbreak took advantage of a vulnerability in Microsoft software. While the company had released a patch for the security loophole back in March, many folks didn't install the update—which left them open to attack. We get that it's hard to stay on top of an ever-growing list of updates from an ever-growing list of software and applications used in your daily life. That's why we recommend changing your settings to enable automatic updating.

Finally, stay informed. One of the most common ways that computers are infected with ransomware is through social engineering. Educate yourself on how to detect phishing campaigns, suspicious websites, and other scams. And above all else, exercise common sense. If it seems suspect, it probably is.

10 Easy Steps to Clean Your Infected Computer

You log onto your computer and it takes forever to boot. When it finally does, a few unfamiliar applications litter your desktop, and your browser immediately sends you to an ad for hair loss products.
Sounds like your PC has a problem with malware.

So what should you do? Before you flip out, try these simple steps to clean up your infected computer.

1. Computer acting suspect? Do a little digging and check for symptoms.
Look for issues characteristic of a malware infection:

- Does your web browser freeze or become unresponsive?
- Do you get redirected to web pages other than the ones you are trying to visit?

- Are you bombarded with pop-up messages?
- Does your computer run slower than usual?
- Do you see new icons on your desktop that you don't recognize?

Unfortunately, even if you see nothing wrong with your computer, there may be trouble brewing under the surface, sneaking around and screwing with your files undetected. So it's a safe bet to move on to Step 2 even if you can't find a symptom.

2. Use protection: Enter safe mode.
Remove CDs and DVDs, and unplug USB drives from your computer. Then shut down.
When you restart, press the F8 key repeatedly. This should bring up the Advanced Boot Options menu.
Select Safe Mode with Networking and press Enter. Only the bare minimum programs and services are used in this mode. If any malware is programmed to automatically load when Windows starts, entering safe mode may block the attempt.

3. Back up your files, including documents, photos, and videos. Especially (haha) cat videos.
Do not back up program files, as those are where infections like to hide. You can always download these programs again if files are lost.

4. Download an on-demand malware scanner such as Malwarebytes Anti-Malware.
Follow set-up instructions and install the program.

5. Disconnect from the Internet. Then run a scan.
If you truly believe you are infected, do not pass go, do not collect $100. Just go directly to the scan. If you do have an infection, your on-demand scanner should let you know that you in danger, girl. A list of scan results tells you what malware was found and removed.

6. Restart your computer. After all, everyone deserves a second chance.

7. Confirm the results of your anti-malware scan by running a full scan with another malware detection program.
Restart again if the program found additional infections.

8. Update your operating system, browser, and applications.
If there's an update available on any of your software, go ahead and do it. Some of the most dangerous forms of malware are delivered by "exploits" that take advantage of out-of-date software.

9. Reset all of your passwords.
Before being deleted, malware could have captured your passwords and forwarded them to hackers. Change each and every password you can think of, and make sure they're strong. None of this 1, 2, 3, 4, 5 business. That's the combination an idiot would use on his luggage.

From Malwarebytes whose software has rescued me from at least one ransomware attack.

ABOUT THE AUTHOR

Wendy Zamora
Head of Content, Malwarebytes Labs
Wordsmith. Card-carrying journalist. Lover of meatballs.

CPR Training

The board of the NPOA held CPR and Stroke recognition training on December 13. It was attended by more than 20 residents. They learned about what to do if someone in your vicinity is in cardiac arrest. The instructors from Moore County informed the residents about the steps to take to help a person in that situation. Here are the steps you should take:

- Make sure the scene is safe
- Check to see if the person is OK – ask him if they are ok
- Check for breathing
- Call 911
- Call for an AED – do you know where AEDs are located in Moore County and more importantly here at National?
- Start CPR – clear the clothes and start chest compressions – make sure the person is on a hard flat surface
- Use the AED – follow the instructions

There is an AED in the NPOA Security vehicle and also one outside the pro shop in the No. 9 clubhouse. Make sure the Security phone number (910-295-4381) and the Clubhouse phone number (910-295-4300) are in your cell phones.
Read the information below about Heartsafe Moore County:

HeartSafe Moore County (HSMC), which formed in November 2007, is a group of community leaders committed to raising awareness of Sudden Cardiac Arrest (SCA).
They are advocates for public access defibrillation (PAD) programs and have one goal – to save lives through early defibrillation.
HSMC's program objectives include ensuring that Automated External Defibrillators (AEDs) are available in all public schools, public recreation areas, churches, businesses, and places where there are large groups of individuals gathered.
Community awareness of SCA and the need for AED's is growing. Currently there are more than 300 registered AED locations in Moore County
The downtown area of Southern Pines is now recognized as one of the first HeartSafe Communities in the state – thanks to a network of publicly accessible AED's located along the downtown sidewalks in cooperation with the Southern Pines Fire Department.

The second half of the program was to inform us about the warning signs of a stroke. Remember the following: **F A S T**

F – Face drooping – ask the person to smile
A – Arm weakness – ask the person to raise their arms
S – Speech difficulty – slurred or garbled or none at all
T – Time to call 911 – check the time when the first symptoms occurred
Other symptoms may include:

- Sudden numbness or weakness of the leg
- Sudden confusion or trouble understanding
- Sudden trouble seeing in one or both eyes
- Sudden trouble walking, dizziness, loss of balance or coordination
- Sudden severe headache with no known cause

In any of these cases call 911 and note the time when the first symptoms occurred. Additional information may be obtained from strokeassociation.org.