

**Topic: Recognizing spam**

When I am done this lesson, I will know:

- What spam is
- How to recognize spam in my mailbox



**Pre and Post Self-Assessment**

	Pre	Pre	Post	Post
	Yes, I know this	No, I want to learn this	Yes, I know this	I still need more practice to learn this
I know what spam is				
I know how to recognize spam in my mailbox				



**New Words and Terms**

database  
 filter  
 hacking  
 Internet Service Provider (ISP)  
 phishing  
 spam  
 spammer

spoofed email



Review

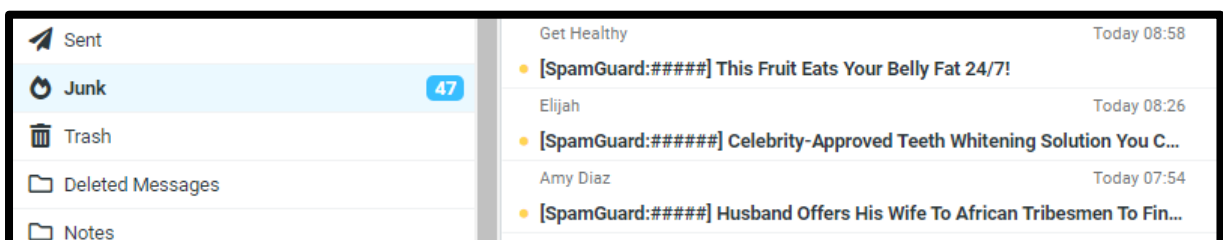
Malware is short for malicious software. This means that while most of us refer to these threats as viruses, the correct catch-all term should indeed be malware. Malicious software comes in many forms, but malware itself is a general term that could be used to describe any number of things, such as viruses, worms, trojans, spyware, and others.

## What is spam?

Spam is digital communication that you do not want or did not sign up for. Spam often comes in the form of an email. However, spam can also be sent through text and social media. Spam can also be posted on blogs or internet forums. Spammers send out communications in bulk to as many emails as possible. Sending out spam is called spamming.

Internet service providers (ISP's) spend money to create filters to keep email spam from getting into your inbox. A filter will catch the spam before it goes to your inbox. It is usually stored in a folder called "Spam", "Junk", or "Junk e-mail". Most junk email is deleted automatically after a set period of time.

Here is an example of what spam can look like in your mailbox:



How do spammers get my email?

Spammers have many different ways to get your email. Here are some of the most common ways:

1. If your email address is on a website a spammer might be able to find it. They write programs that search thousands of websites and make lists of email addresses.
2. Spammers will make up email lists by using a domain and adding common names to it. For example, they might use the domain “gmail.com” and make a list of names that could have that email address such as:
  - o bob.jones@gmail.com
  - o jane.smith @gmail.com
3. Companies sell your information or spammers steal it from a company by hacking into their database
4. Spammers use a method called “phishing”. They get your information by tricking you into signing up for something that isn’t real (a free contest) or pretending that they know you (e.g. a friend request on Facebook)

Source: <https://www.timesheets.com/blog/2015/05/how-spammers-get-email-address-what-to-do-about-it/>

## **Different types of spam**

Not all spam will be filtered out by the ISP so it is important to recognize spam. There are lots of different types of spam. Some spam is annoying but harmless. Other spam can be really serious if the spammers are using it to try to steal from you or spread viruses.

### *Phishing emails*

Phishing emails trick people into giving up information, e.g. website logins, and credit card info, using spoofed emails. Spoofed emails mimic, or spoof, an email from a legitimate sender, demanding some sort of action.

Common types of phishing emails:

- A request for payment of an outstanding invoice.
- A request to reset your password or verify your account.
- Verification of purchases you never made.

- A request for updated billing information.

### *Mobile phone spam*

Spam can be sent to mobile phones as phone calls and texts.

The most common mobile phone scams use pre-recorded messages pretending to be from banks, credit card companies, cable companies, the government, and debt collectors. The calls are often made by robots. Text message scams are often senders trying to sell you something.

### *Malspam*

Malspam is any kind of malware spread using spam. The malware is usually hidden in attachments (e.g. Word or PDF files) which download and spread when you open the attachment.

### *Advance-fee scams*

A mysterious sender sends an email offering you a big reward in exchange for a cash advance, usually as some sort of processing fee, required to unlock the larger sum. Once you wire the cash to the scammer, they disappear with your money.

Source: <https://www.malwarebytes.com/spam/>

### **How do I know it is spam?**

1. The content seems inappropriate or something you would not have signed up for (e.g. adult content).
2. The sender's address does not match the domain for the company they claim to represent. In other words, emails from PayPal always come from

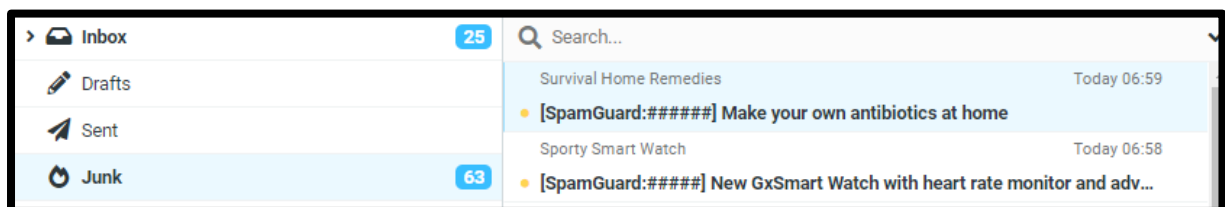
example@paypal.com, and emails from Microsoft always come from example@microsoft.com.

3. The email is addressed to “customer”, “friend” or something else generic, not you personally. Legitimate emails from companies and people you know will usually be addressed to you by name.
4. The email has links embedded that seem unusual or suspicious. If you are still not sure, don’t click on the link. Copy it and paste it into your web browser to check the website out directly. Spam often includes links to spoofed sites designed to capture your login.
5. The email has lots of typos and bad grammar. This often happens when online translators are used by spammers from different countries.
6. The email is too good to be true. Advance-fee scams work this way.
7. There are attachments. Businesses don’t usually send emails with attachments. There are attachments.


Source: <https://www.malwarebytes.com/spam/>

## Review of a Spam Example

Let’s take a look at an example of spam. In the junk email folder, there is a message from “Survival Home Remedies” with the subject line “Make your own antibiotics at home”.



The picture below shows the content of the email when you open it. If you read through it there is at least one spelling mistake, phrases that sound odd, and some words that don’t seem to make sense.

**[SpamGuard:#####] Make your own antibiotics at home** 





From Survival Home Remedies on 2021-04-03 06:59

From Survival Home Remedies

To ritchieg@execulink.com

Date Today 06:59

[All headers...](#)

 [Details](#)  [Plain text](#)



Did you know you can make your own penicilin, at home... using cantaloupe rinds?



In a survival situation where pharmacies are closed (or looted), survival home remedies could be your only hope.

For instance, you can make your own anesthetic at home. [This book](#) shows how to make chloroform at home... a powerful painkiller that can prove essential in a health emergency.

Plus 101 other home remedies for survival situations - in Dr. John Herzog's book that's been an instant hit with preppers and patriots.

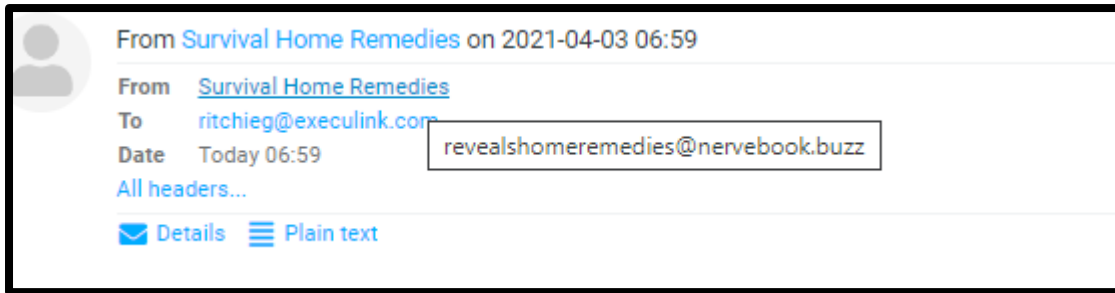
[Click here to find out more about "The Doctor's Book of Survival Home Remedies".](#)



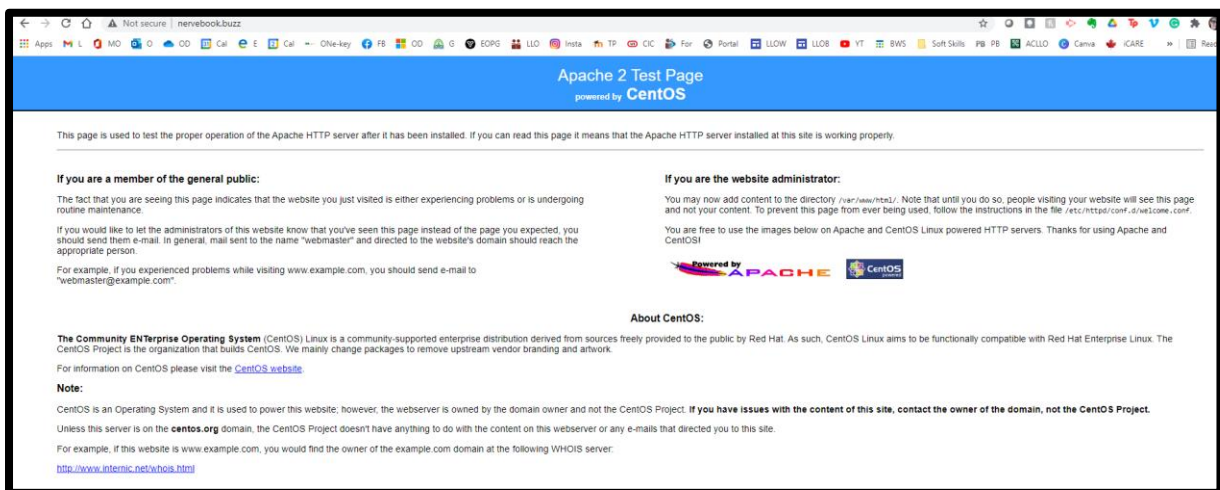
**Discussion Question**

Discuss the parts of this email that don't seem quite right. What specific things can you find that make you think it might be spam?

When you take a closer look at who the email is from you can see the domain is "nervebook.buzz".



When you check the domain “nervebook.buzz” by copyasting it into a browser page appears. This confirms that nervebook.buzz is not a legitimate company.



### How do I stop spam?

1. If you think it might be a spam email, call or text don't open it or answer it! Delete it.
2. If you accidentally answer a call that is from a spanner, never say yes or complete any actions they ask you to do. Hang up and add the number to your blocked numbers list.
3. Make sure you have your email spam filter turned on. Check your spam or junk folder on a regular basis to make sure that any real emails did not get filtered out. If a legitimate email is in your spam or junk folder, you can mark it “not junk” or “not spam” so emails from that address are not filtered out in the future.

4. If you have the option when you are creating accounts online, use multi-factor authentication. With two-factor or multi-factor authentication, even if your username and password are compromised, cybercriminals won't be able to get around the additional authentication requirements on your account. Additional authentication factors include secret questions or verification codes sent to your phone via text message.

Source: <https://www.malwarebytes.com/spam/>



### Discussion Question

1. What are some examples of spam that you have received in the past? What did you do when you received spam?



### Check Your Knowledge

What are two ways you can stop spam?

- 1.
- 2.



### Try this/Practice

Check your junk or spam folder to see if there are any emails in there. Delete them.



### Optional: I Want to Learn More

A small icon of a film strip with a play button in the center.	<p>Watch this video to learn more about avoiding spam and phishing.</p> <p>Source: GCFGlobal</p>	<p><a href="https://edu.gcfglobal.org/en/tr_zh-cn-internet-safety/-spam-and-phishing/1/">https://edu.gcfglobal.org/en/tr_zh-cn-internet-safety/-spam-and-phishing/1/</a></p>
----------------------------------------------------------------	--------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------





### Bridge Adult Literacy Curriculum Framework Connection

Competency	Task Group(s)
Find and Use Information	<ul style="list-style-type: none"><li>● Read Continuous Text (L3 - long sentences, specialized language)</li><li>● Extract Information from Films, Broadcasts, and Presentations</li></ul>
Communicate Ideas and Information	<ul style="list-style-type: none"><li>● Interact with Others (L1 -share information for highly explicit purpose)</li><li>● Writes Continuous Text (L1-Conveys simple ideas and factual information)</li></ul>
Use Digital Technology	<ul style="list-style-type: none"><li>● Open an email program and delete a message from an online folder</li></ul>

[www.bridgela.org](http://www.bridgela.org) 

[info@bridgela.org](mailto:info@bridgela.org) 

(310) 999-0001 