Beware of the 7 most common types of spam

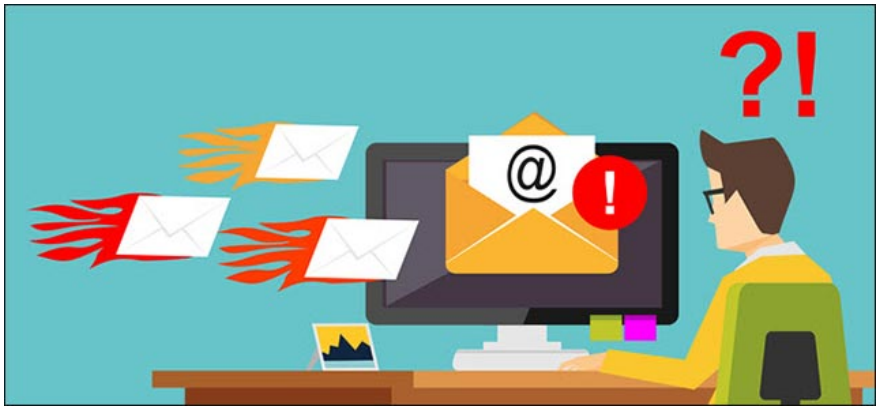
Email, as we know, is always the most vulnerable object on the internet today. Anyone who has ever used email is no stranger to having to spend time 'processing' the spam pile almost regularly.

Email, as we know, is always the most vulnerable object on the internet today. Anyone who has ever used email is no stranger to having to spend time "processing" the spam pile almost regularly. Types of email spam (email spam) not only make us uncomfortable every time we check inboxes, but can also contain risks of fraud or worse, system security. However, if you know how to identify and classify these spam emails, you will limit the risk of becoming a victim of online scams or spreading malicious code.

1. The most effective spam blocking tips

Spam is not only a nuisance, but it also involves many other complex activities on the internet. According to security researchers, an estimated 560 billion spam messages are sent every day on e-mail platforms, accounting for 91% of the total number of emails sent and received daily on Around the world. Although only a small percentage of spam recipients fall victim to scams, the world has lost nearly $ 500 million a year through the FBI's research. Spam-based cybercrime activity. This is equivalent to about 26,000 spam phishing complaints every month, meaning a complaint is sent every 100 seconds.

To protect yourself against spam phishing activities, the prerequisite is that you need to know some basic information about the form and characteristics of spam types. Of course, modern anti-virus or email filters can also help you deal effectively with spam, but equipping yourself with different types of spam, such as email scams death, fake email, Nigerian fraud, or pornography, is the first step to protecting yourself. In addition, understanding when to reject a 'great' offer (and possibly a scam), or check if the message is from a real business or just a fraud wanting to infect malicious code on your system is also a very useful factor, especially in case you often have to work with email.



1. 11 rules for professional email writing that everyone needs to remember

In principle, when you receive a suspicious email, you must always consider carefully the content and suggestions in it to see if there are any unusual factors. Then check the authenticity of any URL or attachments in the mail before deciding to disclose any personal information, passwords or money. By using the following tips, you will fully master the ability to identify different types of spam, and protect yourself against any malicious actions via email. Remember, protect yourself with knowledge before resorting to any security tool, crooks will not have the opportunity to deceive a wise and alert person.

7 types of common spam

1. Unexpected advertising messages
2. Email fraud (phishing email)
3. Email Trojan
4. Email chain
5. Fake email (email Spoofing)
6. Virus infection scam
7. Spam about pornography

Unexpected advertising messages

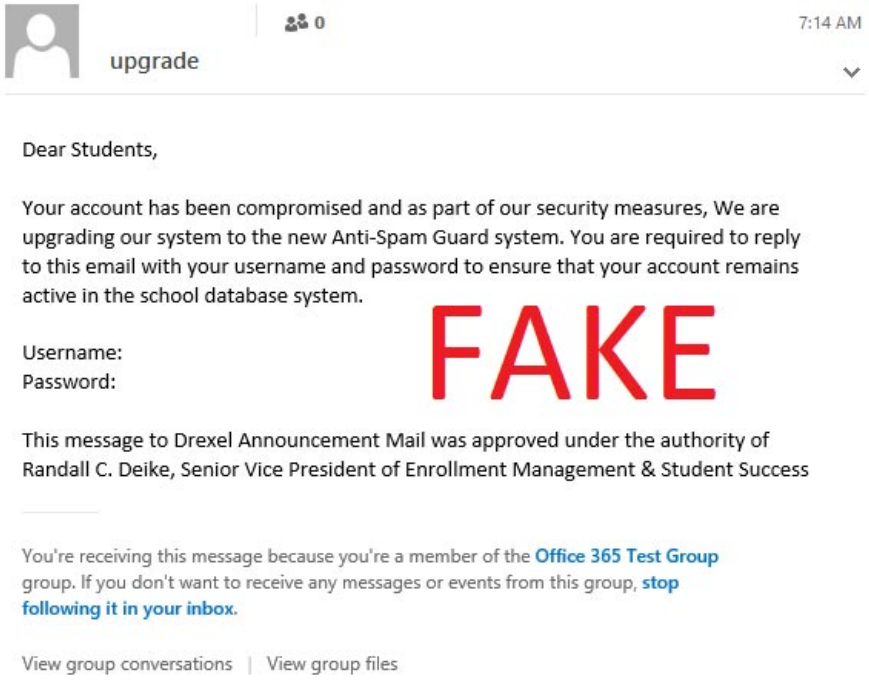
Unwanted email ads are the most common type when it comes to spam, which feels quite uncomfortable because of being in the spam section, but they usually account for a huge amount. There are hundreds of billions of

unwanted advertising messages sent every day, mostly information about miraculous weight-loss drugs, physiological enhancement products for men, travel programs, promotions, or research program, online chemistry. In general, advertising spam is often sent blameless and the recipient is a very long list coming from certain individuals or groups, and the quality of this type of spam is often quite low. Sometimes, it leads people to be light-hearted, find ways to read their credit card numbers and personal information.

This type of spam is often repeated dozens of times for a personal mailbox, why is that? One reason is that advertisers want to use psychological effects. When certain product images keep hitting the reader's eyes, it is time to buy something with the same function (or the same type), the brand image of that spam will appear in the person's head first. . Another reason is to stimulate the curiosity of email users who want to read a promotional message to see if the content is beneficial to them.

1. How to change the default font for Mail application on Windows 10

Email fraud (phishing email)



Phishing email is the second most popular type of spam on email platforms, and is also one of the most difficult to detect spam types. Phishing emails are often designed to simulate the prototype of real email, sent from reputable organizations and businesses (such as Amazon, Google, Microsoft, or Facebook .) to deceive users into clicking Go to the link or download the attachment. This link will redirect the victim to a phishing site (also designed to look like the real thing). Here, the victim will continue to be tricked into entering their account information, passwords, and personal information. This data is then used by cyber criminals to infiltrate and hijack the victim's real account. As for the case of phishing emails attached to malicious files, if users download this file to their computer, their system will be infected with malicious information stealing.

In general, phishing emails are a very large and complex category. If you want to delve deeper into phishing emails, please continue to refer to our 'How to identify phishing emails' article.

1. 7 most popular email security protocols today

Email Trojan

You must first know what a Trojan is. A Trojan horse, also known as a Trojan, is a malicious code or malware that looks legitimate at first, but in fact it can completely take control of the victim's computer. The goal of creating a Trojan is to damage, destroy, steal information, or generally say, to perform harmful actions on targeted data or network systems.

Trojans have been associated with email for a long time and still give extremely high efficiency. More dangerous, Trojans not only infect victims' computers, but also have the ability to automatically send malicious code-spreading emails to anyone in the victim's contact list. The most well-known Trojan-spread spread Trojan, named '2000 ILOVEYOU, has stalled millions of people around the world. It beats each individual's psychological curiosity and when the user opens and downloads malicious files, this attachment will damage the local computer system and resume sending malicious emails to all. people on the list of new victims. As such, the malicious code spreads exponentially, causing damage on a very large scale.

1. 2 ways to hide your email address on a website

Email chain

Another kind of junk email struck the curious psychology of the users. Often the email chain will tell interesting stories and convince you to convey the message to others, otherwise you will be forced to do, or suffer from some very serious consequences. Although this type of spam has been around for a long time and has been widely condemned, there are still people who lack vigilance to become victims of it.

Fake email (email Spoofing)

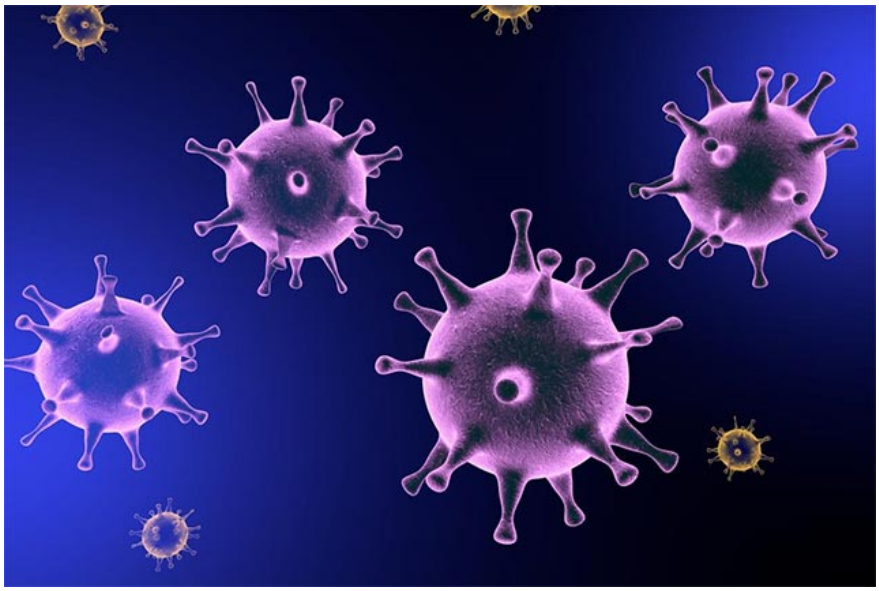
Quite similar to phishing emails, but instead of using a technique to make spam methods more reliable, many spammers will proceed to send messages that seem to come from an address. email is different from reality. Basically, email Spoofing is the creation of email messages with a fake sender address. Because the core email protocols do not have any authentication mechanisms. In general, it will try to tamper with the recipient of the

origin of the message. This identity theft technique gives the impression that phishing emails come from a trusted source, company or organization.

There are many tricks to create sophisticated phishing emails, such as the message "Your account has been compromised!" or "Amazon has a package ready to send you" - phishing emails that are difficult to distinguish.

1. [Infographic] 4 types of Phishing are easy to trap users

Virus infection scam



Of course no one wants to be a victim of the virus. So, when I received an email saying my computer was infected with a virus, users would often be confused and believe in this baseless notification, and turn themselves into victims of another form of spam. . Next, the victim will fall into the trap and download software that is advertised as an anti-virus tool, but in fact they have 'pumped' their computer with real viruses. There is also another variation of this form of junk email, that crook will infect the victim's system and ask them to pay for the acquisition of specific anti-virus software. Email phishing scams are a branch of phishing emails, but are quite popular and relatively dangerous.

1. The best anti-spam mail programs - Part I

Spam about pornography

Distributing or cheating on pornography is one of the worldwide popular activities. They are not only used on email, but also appear on social networking platforms, or rather every corner of the internet. Any trick related to pornography is one of the most popular forms of malware distribution by hackers worldwide. Porn spammers often collect or buy email addresses from people, send full T&A notifications that redirect victims directly to adult websites filled with malicious content, malicious code, viruses , Trojan, to content that violates social norms.

Above is the definition as well as characteristics of 7 types of spam that are commonly used on current email platforms. Hopefully these little information will help you be more alert to these 'old but not old' scams.