**SPAM NATION -Secrets that you don’t know about Spam industry**

Have you ever opened an email you thought was safe, only to find a virus attached? Or clicked on a cat video, only to have your computer paralyzed by malicious software? Cybercriminals are laughing all the way to the bank. Spam is a serious threat, and no one is safe. But who exactly are spammers, and how do they go about earning millions from sending endless streams of fake pharmaceutical advertisements and get-rich-quick schemes? These blinks will show you the dark corners of the internet where cybercriminals organize their activities and are always one step ahead of the law. Yes, anti-spammers are fighting back, but it’s still up to you to get savvy on how to spot a spammer and stay safe. In the following blinks, you’ll discover

* why you should never buy prescription drugs over the internet;
* why the government hit Google with a $500 million fine;
* why you shouldn’t open random emails, even when it says it’s from the IRS.

Try our miracle sex pill! Lose 30 pounds with this no-risk diet! Almost daily we’re inundated with spam emails, touting everything from hot dates to how-to-be-a-millionaire scams. It’s easy to laugh these emails off as harmless, if not annoying, marketing ploys. Yet spam is actually a huge industry and poses a serious threat to our safety online. What’s more, even if you never open a spam email or click on a flashy banner ad, the danger is still there. Spam emails often contain viruses and other malware (malicious software) that can infect your computer. In fact, the amount of malware spread via spam is staggering. Companies that produce antivirus solutions claim that they deal with some 82,000 new variants of malware through spam emails every day. During the first quarter of 2013 alone, McAfee, one of the world’s leading computer security companies, discovered some 14 million new malware viruses.

Even worse, malicious software imbedded in spam can turn a computer into a hired gun for cybercrime. Fake ads for Viagra or penis enlargement pills are often set by criminals to snare a computer user, whose hardware is essentially hijacked and added to a sophisticated network of other hijacked computers called a botnet. A botnet can then be hired out to cybercriminals to perform distributed denial of service (DDoS) attacks. During a DDoS attack, a website is bombarded with so much data that it becomes unavailable to users. Such attacks are often performed as part of an extortion scheme, in which a site or group of sites are kept offline until its owner pays a ransom. Sometimes DDoS attacks are even directed at governments, and the consequences can be dire. In 2008, the Estonian government was the target of a massive DDoS attack, and most government websites were down for days. Many of the country’s online banking services went briefly offline, and the national network used for medical emergencies was likewise disrupted.

The spam industry is a highly efficient and profitable machine, run by only a handful of experienced cybercriminals, often with a background in other criminal activities. So who are these people and how do they operate? Among the most important players in the spam world is a man named Pavel Vrublevsky, also known as “Red Eye.” Vrublevsky made a name for himself early on from his profitable network of hard-core porn sites that specialized in depicting scenes of rape, bestiality, incest and other violent material. He also cofounded a spammers’ online forum called Crutop.nu, where members can share trade secrets. “Red Eye” is also the man behind ChronoPay, a payment service that has processed transactions for various cybercrime schemes. Among other rackets, ChronoPay secured payment processing for networks that peddled fake anti-virus software. After Vrublevsky was arrested in 2011, however, these networks fell apart practically overnight. According to computer security company McAfee, their disappearance resulted in a 60-percent drop in reported problems regarding fake anti-virus software. Ironically, Vrublevsky’s career in facilitating cybercrime ran parallel to his tenure as the chairman of an anti-spam initiative spearheaded by the Russian Ministry of Telecommunications. In the early 2000s, a few major players in the spam industry entered partnerships, or partnerkas, which matched spammers with businesses interested in selling illegal products and services. These partnerships have helped spammers to create stable and profitable networks. The partnerkas are involved in several aspects of online scams, taking care of setting up web servers, creating web content, coordinating suppliers and offering customer service. One major partnerka was Rx-Promotion, a venture founded by Vrublevsky and Yuri “Hellman” Kabayenkov, established to set up illegal online pharmacies.

The amount of spam in daily circulation is mind-boggling. However, this flood can be traced back to just a small gang of dedicated spammers. Armed with huge networks of hacked computers, these few cybercriminals provide the firepower of the spam industry. But who exactly are these spammers? One major player is a Russian named Dmitri Nechvolod, also know as “Gugle,” who was behind the Cutwail botnet – one of the largest and most damaging botnets of all time. In 2008, the Cutwail botnet infected more than 125,000 computers and was capable of pumping out 16 billion spam messages per day. To put this in perspective, the total number of spam messages sent daily worldwide in 2013 was estimated to be about 85 billion. As the Cutwail botnet grew, Nechvolod began hiring other programmers, luring them away from legitimate businesses into a life of cybercrime. According to business partner Igor Vishnevsky, Nechvolod lived a life of luxury. So lavish, in fact, that when he wrecked his $100,000 Lexus, he simply went out and bought a new BMW. Another spam kingpin uses the nickname “Cosma.” This is the man behind the Rustock botnet created in 2006, which in one short year infected approximately 150,000 computers. At its peak, the Rustock botnet could fire off about 30 billion spam messages per day, and it made Cosma rich. Leaked information from ChronoPay shows that in 2010, Cosma received $200,000 in commission, just for his work promoting pharmacy websites for Rx-Promotion. And that was only one of many partnerkas that Cosma was involved in at the time.

If you suffer from a serious disease, managing expensive medications can add to the stress. Yet imagine the relief you might feel if one day, you received an email offering you a version of your medication for a fraction of the original cost. Wouldn’t you be tempted to accept the offer? If so, you’re certainly not alone. In the United States and in other countries, prescription drugs can be expensive; and for the uninsured, shouldering out-of-pocket costs for necessary medication can be almost impossible. At their peak, online “rogue” pharmacies sold prescription medicines to hundreds of thousands of customers worldwide. Take the example of Craig S., a former life-insurance salesman who, when his employer pulled him off his health care plan, decided to buy a generic version of his medication from an online pharmacy. While pills from a regular pharmacy would have cost Craig $212 per month, the online provider offered him the generic equivalent for $178 dollars for a three months’ supply. Such “rogue” pharmacies quickly developed into serious businesses with quality customer support and generous return policies. Researchers at the University of California in San Diego found that some 38 percent of revenue for SpamIt, a pharma partnerka run by Pavel Vrublevsky’s nemesis Igor Gusev, came from returning customers. Evidently, “rogue” pharma was giving legit pharma a run for its money. However, not all of these pharmacies were on the level. While many served customers well, others sold fake pills, even poisonous ones. For example, in 2006 Marcia Bergeron died as a result of poison that was mixed into the medications she had bought from a rogue pharmacy. An autopsy revealed that she had been slowly poisoned by metals in the pills (which also contained uranium, a radioactive substance) that were used in place of other non-active ingredients.

As the rogue pharma business grew, spam kingpins Igor Gusev and Pavel Vrublevsky became richer. Yet their growing wealth and power was accompanied by paranoia and distrust. Very soon the two spammers began to loathe one another, eventually leading to a serious fallout. The feud between Gusev and Vrublevsky, now known as the Pharma Wars, was as vicious as it was costly. As Gusev, the man behind the spam pharma partnerkas GlavMed and SpamIt, was vacationing in Spain in 2008, he received troubling messages from a hacker friend back in Russia. His friend had run into one of Vrublevsky’s business partners, who, while drunk, had boasted of initiating a criminal investigation against Gusev with the aim of putting him behind bars. Gusev retaliated in a big way. Chat records from 2010 reveal that he spent over $400,000 bribing law enforcement officials to both protect himself and convince police to go after Vrublevsky. His money ended up being well spent, as Vrublevsky was sentenced to two-and-a-half years in prison. But Gusev couldn’t hide his criminal activities forever. Under pressure from the law, he was eventually forced to close down SpamIt and flee the country. As some top spammers tell it, this bitter feud was ruinous for the spam industry. Not only did the Pharma Wars cost spammers and partnerkas lots of money, but it also attracted the attention of politicians and law enforcement agencies, forcing spammers to abandon their profitable businesses in search of new turf.

In the spam wars, there are good guys and bad guys. The good guys are anti-spam activists, or “antis,” who work to curb cybercriminals and their activities – often at risk to themselves personally. Anti-spam start-up Blue Security came up with ingenious ways to shut down spammers, but their campaign came at a high price. The company developed software called Blue Frog, which when used, would protect a user from spam by sending a request email back to the email sender’s network. The request was a simple one: Please don’t send any more junk email. Blue Security noticed however that many of these messages were simply ignored, so they devised a new scheme. Instead of receiving a request from a single user, a spammer’s inbox would be flooded with requests from all of Blue Security’s 522,000 users simultaneously, creating such heavy traffic . that a spammer would effectively have his email system shut down. The spammers retaliated in a more criminal fashion. One of Blue Security’s founders was anonymously sent pictures of his children on the playground – a clear threat. Under this kind of pressure, the start-up’s main investor pulled out, and the company shut down. One of the difficulties in fighting spammers is that they often join forces to attack those who get in their way. In 2013, a non-profit focused on tracking spammers called Spamhaus suffered what some experts have called the largest concerted cyberattack in the history of the internet. A group of cybercriminals bombarded the Spamhaus website with over 300 billion bits of data per second for over 90 days. The data didn’t just affect Spamhaus, however; hundreds of millions of internet users also experienced delays and error messages. Sven Olaf Kamphuis, a 35-year-old man from Holland, was later arrested in Spain for his involvement in coordinating the attack.

While we might expect the government to coordinate the fight against spam and cybercrime, private companies also have an important role to play. Some are even leading successful efforts. Credit card companies, for example, have made serious changes to general protocols as a means of protecting themselves and their customers against cybercrime. In 2012, Visa introduced changes to their regulations regarding the sale of pharmaceutical-related products. These sales are now considered “high risk,” and issuing new contracts for payment processing to a high-risk company requires a higher standard of due diligence. Among other things, companies that sell pharmaceuticalrelated products are required to have $100 million in equity and a good risk-management score. In addition to making the barrier for entry harder for illicit businesses, companies that aid illegal activity online now face punishment. The domain registrar EstDomains, which for many years had been a favorite among spammers and online scammers, had its accreditation revoked in 2008 after a story in The Washington Post revealed that CEO Vladimir Tsastsin had previously been convicted of credit card fraud and money laundering. As a result, many other registrars that previously had not considered it necessary to track how customers used their domains have now begun to screen potential customers. And in 2011, the U.S. Justice Department announced that Google had agreed to pay a $500 million fine to settle an ongoing criminal investigation, which alleged that the online giant had allowed rogue pharmacies to advertise their products in the American market. The enormous size of the fine was meant to represent the profit Google had made from hosting the ads.

Spammers and their kin always seem one step ahead of the law. To be sure, cybercriminals never rest, and no one is safe. The efforts of companies like Microsoft and various law enforcement agencies have made it much more difficult for cybercrime partnerships to access credit card processing through payment services such as ChronoPay. These tighter regulations have effectively killed the fake anti-virus software industry. Yet in this void, a new threat has emerged: ransomware. In a ransomware scheme, victims receive emails or pop-up messages that appear as if they’re from the Federal Bureau of Investigation or the U.S. Department of Homeland Security. The messages claim that the user has committed a crime, such as downloading pirated content or child pornography, and that they must pay a fine to avoid prosecution. Usually, victims are instructed to pay the fine using a prepaid debit card or cash voucher, to make it harder to trace the money. At the same time, the victim’s computer is locked down and infected with software that encrypts all the files on the computer, denying the user access until he pays or manages to remove the virus. Botnets too are much more malicious than they were in the past. The Rustock botnet, which was one of the most active pharmacy site promoters during the height of the Pharma Wars, now spreads malware designed to harvest passwords or other sensitive information. These spam messages take many forms, such as fake FedEx messages or Internal Revenue Service audits. They target small and midsized companies, hoping to grab usernames and passwords from company employees in charge of financial transactions. Armed with this information, cybercriminals can either make payments to their own accounts or sell the information to other cybercriminals.

The key message in this book: Those spam emails in your inbox are far more than a nuisance. In fact, they’re part of an industry run by a few powerful cybercriminals and represent a direct threat to everyone, even if you’ve never opened a single spam email.

Actionable advice: Nothing is more precious than your password. Too many people are lazy when it comes to creating good passwords. You should strive to make your passwords as difficult to crack as possible. Ensure your password is over ten characters if possible, and combine both numbers, letters and special characters.