



SPAM SCAMS

Filter Tips: 10 Scams to Screen from Your Email

While some consumers find unsolicited commercial email — also known as “spam” — informative, others find it annoying and time consuming. Still others find it expensive: They’re among the people who have lost money to spam that contained bogus offers and fraudulent promotions.

Many Internet Service Providers and computer operating systems offer filtering software to limit the spam in their users’ email inboxes. In addition, some old-fashioned ‘filter tips’ can help you save time and money by avoiding frauds pitched in email. OnGuard Online wants computer users to screen spam for scams, send unwanted spam on to the appropriate enforcement authorities, and then hit delete. Here’s how to spot 10 common spam scams:

1. The “Nigerian” Email Scam

The Bait: Con artists claim to be officials, businesspeople, or the surviving spouses of former government honchos in Nigeria or another country whose money is somehow tied up for a limited time. They offer to transfer lots of money into your bank account if you will pay a fee or “taxes” to help them access their money. If you respond to the initial offer, you may receive documents that look “official.” Then they ask you to send money to cover transaction and transfer costs and attorney’s fees, as well as blank letterhead, your bank account numbers, or other information. They may even encourage you to travel to the country in question, or a neighboring country, to complete the transaction. Some fraudsters have even produced trunks of dyed or stamped money to try to verify their claims.

The Catch: The emails are from crooks trying to steal your money or your identity. Inevitably, in this scenario, emergencies come up, requiring more of your money and delaying the “transfer” of funds to your account. In the end, there aren’t any profits for you, and the scam artist vanishes with your money. The harm sometimes can be felt even beyond your pocketbook: according to State Department reports, people who have responded to “pay in advance” solicitations have been beaten, subjected to threats and extortion, and in some cases, murdered.

Your Safety Net: If you receive an email from someone claiming to need your help getting money out of a foreign country, don’t respond.

Forward “Nigerian” scams — including all the email addressing information — to spam@uce.gov. If you’ve lost money to one of these schemes, call your local Secret Service field office. Local field offices are listed in the Blue Pages of your telephone directory.



SPAM SCAMS

2. Phishing

The Bait: Email or pop-up messages that claim to be from a business or organization you may deal with — say, an Internet service provider (ISP), bank, online payment service, or even a government agency. The message may ask you to “update,” “validate,” or “confirm” your account information or face dire consequences.

The Catch: Phishing is a scam where Internet fraudsters send spam or pop-up messages to reel in personal and financial information from unsuspecting victims. The messages direct you to a website that looks just like a legitimate organization’s site, or to a phone number purporting to be real. But these are bogus and exist simply to trick you into divulging your personal information so the operators can steal it, fake your identity, and run up bills or commit crimes in your name.

Your Safety Net: Make it a policy never to respond to emails or pop-ups that ask for your personal or financial information, click on links in the message, or call phone numbers given in the message. Don’t cut and paste a link from the message into your Web browser, either: phishers can make links look like they go one place, but then actually take you to a look-alike site. If you are concerned about your account, contact the organization using a phone number you know to be genuine, or open a new Internet browser session and type in the company’s correct Web address yourself. Using anti-virus and anti-spyware software and a firewall, and keeping them up to date, can help.

Forward phishing emails to spam@uce.gov and to the organization that is being spoofed.

3. Work-at-Home Scams

The Bait: Advertisements that promise steady income for minimal labor — in medical claims processing, envelope-stuffing, craft assembly work, or other jobs. The ads use similar come-ons: Fast cash. Minimal work. No risk. And the advantage of working from home when it’s convenient for you.

The Catch: The ads don’t say you may have to work many hours without pay, or pay hidden costs to place newspaper ads, make photocopies, or buy supplies, software, or equipment to do the job. Once you put in your own time and money, you’re likely to find promoters who refuse to pay you, claiming that your work isn’t up to their “quality standards.”

Your Safety Net: The FTC has yet to find anyone who has gotten rich stuffing envelopes or assembling magnets at home. Legitimate work-at-home business promoters should tell you — in writing — exactly what’s involved in the program they’re selling. Before you commit any money, find out what tasks you will have to perform, whether you will be paid a salary or work on commission, who will pay you, when you will get your first paycheck, the total cost of the



SPAM SCAMS

program — including supplies, equipment and membership fees — and what you will get for your money. Can you verify information from current workers? Be aware of “shills,” people who are paid to lie and give you every reason to pay for work. Get professional advice from a lawyer, an accountant, a financial advisor, or another expert if you need it, and check out the company with your local consumer protection agency, state Attorney General and the Better Business Bureau — not only where the company is located, but also where you live.

Forward work-at-home scams to spam@uce.gov.

4. Weight Loss Claims

The Bait: Emails promising a revolutionary pill, patch, cream, or other product that will result in weight loss without diet or exercise. Some products claim to block the absorption of fat, carbs, or calories; others guarantee permanent weight loss; still others suggest you’ll lose lots of weight at lightening speed.

The Catch: These are gimmicks, playing on your sense of hopefulness. There’s nothing available through email you can wear or apply to your skin that can cause permanent — or even significant weight loss.

Your Safety Net: Experts agree that the best way to lose weight is to eat fewer calories and increase your physical activity so you burn more energy. A reasonable goal is to lose about a pound a week. For most people, that means cutting about 500 calories a day from your diet, eating a variety of nutritious foods, and exercising regularly. Permanent weight loss happens with permanent lifestyle changes. Talk to your health care provider about a nutrition and exercise program suited to your lifestyle and metabolism.

Forward weight loss emails to spam@uce.gov.

5. Foreign Lotteries

The Bait: Emails boasting enticing odds in foreign lotteries. You may even get a message claiming you’ve already won! You just have to pay to get your prize or collect your winnings.

The Catch: Most promotions for foreign lotteries are phony. The scammers will ask you to pay “taxes,” “customs duties,” or fees — and then keep any money you send.” Scammers sometime ask you to send funds via wire transfer. Don’t send cash or use a money-wiring service because you’ll have no recourse if something goes wrong. In addition, lottery hustlers use victims’ bank account numbers to make unauthorized withdrawals or their credit card numbers to run up additional charges. And one last important note: participating in a foreign lottery violates U.S. law.



SPAM SCAMS

Your Safety Net: Skip these offers. Don't send money now on the promise of a pay-off later.

Forward solicitations for foreign lottery promotions to spam@uce.gov.

6. Cure-All Products

The Bait: Emails claiming that a product is a “miracle cure,” a “scientific breakthrough,” an “ancient remedy” — or a quick and effective cure for a wide variety of ailments or diseases. They generally announce limited availability, and require payment in advance, and offer a no-risk “money-back guarantee.” Case histories or testimonials by consumers or doctors claiming amazing results are not uncommon.

The Catch: There is no product or dietary supplement available via email that can make good on its claims to shrink tumors, cure insomnia, cure impotency, treat Alzheimer's disease, or prevent severe memory loss. These kinds of claims deal with the treatment of diseases; companies that want to make claims like these must follow the FDA's pre-market testing and review process required for new drugs.

Your Safety Net: When evaluating health-related claims, be skeptical. Consult a health care professional before buying any “cure-all” that claims to treat a wide range of ailments or offers quick cures and easy solutions to serious illnesses. Generally speaking, a cure all is a cure none.

Forward spam with miracle health claims to spam@uce.gov.

7. Check Overpayment Scams

The Bait: A response to your ad or online auction posting, offering to pay with a cashier's, personal, or corporate check. At the last minute, the so-called buyer (or the buyer's “agent”) comes up with a reason for writing the check for more than the purchase price, and asks you to wire back the difference after you deposit the check.

The Catch: If you deposit the check, you lose. Typically, the checks are counterfeit, but they're good enough to fool unsuspecting bank tellers and increase the balance in your bank account — temporarily. But when the check eventually bounces, you are liable for the entire amount.

Your Safety Net: Don't accept a check for more than your selling price, no matter how tempting the plea or convincing the story. Ask the buyer to write the check for the purchase price. If the buyer sends the incorrect amount, return the check. Don't send the merchandise. As a seller who accepts payment by check, you may ask for a check drawn on a local bank, or a bank with a local branch.



SPAM SCAMS

That way, you can visit personally to make sure the check is valid. If that's not possible, call the bank the check was drawn on using the phone number from directory assistance or an Internet site that you know and trust, not from the person who gave you the check. Ask if the check is valid.

Forward check overpayment scams to spam@uce.gov and your state Attorney General. You can find contact information for your state Attorney General at www.naag.org.

8. Pay-in-Advance Credit Offers

The Bait: News that you've been "pre-qualified" to get a low-interest loan or credit card, or repair your bad credit even though banks have turned you down. But to take advantage of the offer, you have to ante up a processing fee of several hundred dollars.

The Catch: A legitimate pre-qualified offer means you've been selected to *apply*. You still have to complete an application and you can still be turned down. If you paid a fee in advance for the promise of a loan or credit card, you've been hustled. You might get a list of lenders, but there's no loan, and the person you've paid has taken your money and run.

Your Safety Net: Don't pay for a promise. Legitimate lenders never "guarantee" a card or loan before you apply. They may require that you pay application, appraisal, or credit report fees, but these fees seldom are required before the lender is identified and the application is completed. In addition, the fees generally are paid to the lender, not to the broker or person who arranged the "guaranteed" loan.

Forward unsolicited email containing credit offers to spam@uce.gov.

9. Debt Relief

The Bait: Emails touting a way you can consolidate your bills into one monthly payment without borrowing; stop credit harassment, foreclosures, repossessions, tax levies and garnishments; or wipe out your debts.

The Catch: These offers often involve bankruptcy proceedings, but they rarely say so. While bankruptcy is one way to deal with serious financial problems, it's generally considered the option of last resort. The reason: it has a long-term negative impact on your creditworthiness. A bankruptcy stays on your credit report for 10 years, and can hurt your ability to get credit, a job, insurance, or even a place to live. To top it off, you will likely be responsible for attorneys' fees for bankruptcy proceedings.

Your Safety Net: Read between the lines when looking at these emails. Before resorting to bankruptcy, talk with your creditors about arranging a modified payment plan, contact a credit



SPAM SCAMS

counseling service to help you develop a debt repayment plan, or carefully consider a second mortgage or home equity line of credit. One caution: While a home loan may allow you to consolidate your debt, it also requires your home as collateral. If you can't make the payments, you could lose your home.

Forward debt relief offers to spam@uce.gov.

10. Investment Schemes

The Bait: Emails touting “investments” that promise high rates of return with little or no risk. One version seeks investors to help form an offshore bank. Others are vague about the nature of the investment, but stress the rates of return. Promoters hype their high-level financial connections; the fact that they're privy to inside information; that they'll guarantee the investment; or that they'll buy it back. To close the deal, they often serve up phony statistics, misrepresent the significance of a current event, or stress the unique quality of their offering. And they'll almost always try to rush you into a decision.

The Catch: Many unsolicited schemes are a good investment for the promoters, but not for participants. Promoters of fraudulent investments operate a particular scam for a short time, close down before they can be detected, and quickly spend the money they take in. Often, they reopen under another name, selling another investment scam.

Your Safety Net: Take your time in evaluating the legitimacy of an offer: The higher the promised return, the higher the risk. Don't let a promoter pressure you into committing to an investment before you are certain it's legitimate. Hire your own attorney or an accountant to take a look at any investment offer, too.

Forward spam with investment-related schemes to spam@uce.gov.

Fighting Back

Con artists are clever and cunning, constantly hatching new variations on age-old scams. Still, skeptical consumers can spot questionable or unsavory promotions in email offers. Should you receive an email that you think may be fraudulent, forward it to the FTC at spam@uce.gov, hit delete, and smile. You'll be doing your part to help put a scam artist out of work.

OnGuardOnline.gov provides practical tips from the federal government and the technology industry to help you be on guard against Internet fraud, secure your computer, and protect your personal information.

February 2008