Recognizing and Avoiding Email Scams

US-CERT

Summary

Email provides us a convenient and powerful communications tool. Unfortunately, it also provides scammers and other malicious individuals an easy means for luring potential victims. The scams they attempt run from old-fashioned bait-and-switch operations to phishing schemes using a combination of email and bogus web sites to trick victims into divulging sensitive information. To protect yourself from these scams, you should understand what they are, what they look like, how they work, and what you can do to avoid them. The following recommendations can minimize your chances of falling victim to an email scam:

- Filter spam.
- Don't trust unsolicited email.
- Treat email attachments with caution.
- Don't click links in email messages.
- Install anti-virus software and keep it up to date.
- Install a personal firewall and keep it up to date.
- Configure your email client for security.

These recommendations are explained in the section "What You Can Do to Avoid Becoming a Victim." Ignoring them may leave you vulnerable to identity theft, information theft, the abuse of your computer for illegal activity, the receipt of bogus or illegal merchandise, and financial loss.

Recognizing Email Scams

Unsolicited commercial email, or "spam," is the starting point for many email scams. Before the advent of email, a scammer had to contact each potential victim individually by post, fax, telephone, or through direct personal contact. These methods would often require a significant investment in time and money. To improve the chances of contacting susceptible victims, the scammer might have had to do advance research on the "marks" he or she targeted.

Email has changed the game for scammers. The convenience and anonymity of email, along with the capability it provides for easily contacting thousands of people at once, enables scammers to work in volume. Scammers only need to fool a small percentage of the tens of thousands of people they email for their ruse to pay off. For tips on reducing spam in your email in-box, see US-CERT Cyber Security Tip ST04-007, "Reducing Spam": http://www.us-cert.gov/cas/tips/ST04-007.html

The following sections provide information to help you spot an email scam when it lands in your mailbox. They describe some, but by no means all, of the many email-based scams you're likely to encounter. Armed with this information, you will better recognize email scams, even those not specifically mentioned here.

"Old-fashioned" Fraud Schemes

Many email scams have existed for a long time. In fact, a number of them are merely "recycled" scams that predate the use of email. The FTC has a list of the 12 most common (http://www.ftc.gov/bcp/conline/pubs/alerts/doznalrt.htm). The list includes

- bogus business opportunities
- chain letters
- work-at-home schemes
- health and diet scams
- effortless income
- "free" goods
- investment opportunities
- bulk email schemes
- cable descrambler kits
- "guaranteed" loans or credit

The following sections describe some common fraud schemes initiated through email.

Bogus Business Opportunities

These scams promise the opportunity to make a great deal of money with very little effort. They're normally full of enticements such as "Work only hours a week," "Be your own boss," "Set your own hours," and "Work from home." The email offering these "opportunities" often have subject lines that look like the following:

- Make a Regular Income with Online Auctions
- Get Rich Click
- Put your computer to work for you!
- Use the Internet to make money
- eBay Insider Secrets Revealed 6228

In most cases, the email gives very little detail about the nature of the business opportunity. Most provide an address or web site from which you can, for a fee, obtain an "information kit" about the opportunity. These opportunities, however, usually amount to nothing more than pyramid schemes in which the "opportunity" involves your ability to recruit more unsuspecting people to buy into the scam. Eventually, the scam is uncovered or the pool of new recruits runs dry and it fails.

Health and Diet Scams

Health and diet scams prey on the insecurities some people have about the state of their well-being. These insecurities make some people particularly susceptible to the scams because they may be reluctant or embarrassed to discuss their problems with a doctor, or they can't afford to

buy legitimate drugs or treatment. The scams attempt to lure consumers with promises of quick fixes and amazing results, discount pricing, fast delivery, waived prescription requirements, privacy, and discreet packaging. The email offering these items will have subject lines that look like the following:

- Need to lose weight for summer?
- Increase Your Sexual Performance Drastically
- CONTROL YOUR WEIGHT!!
- Natural Health Remedy That Works!
- Reduce body fat and build lean muscle without exercise
- Young at any age
- Takes years off your appearance
- Gives energy and burns fat

Though they may be backed by customer testimonials, beware: the products don't work.

Discount Software Offers

These scams frequently consist of advertisements for cheap versions of commercial software like Windows XP or Photoshop. The discounts offered may be hard to believe, and with good reason: the scammers either do not deliver the promised software at all, or provide illegal, pirated versions preloaded with Trojan horse software the scammer or other malicious individuals can use to exploit your computer and the information it contains.

419 Advanced Fee Fraud

These schemes are quite elaborate and despite their somewhat preposterous appearance manage to hook a surprising number of victims. Essentially, these scams attempt to entice the victim into a bogus plot to acquire and split a large sum of cash.

Many perpetrators of this kind of fraud have been Nigerian citizens. Consequently, the name "419 scheme" is taken from the section of the Nigerian penal code that addresses fraud.

419 scams are recognizable by their subject lines, which frequently call for an urgent response or refer to a personal introduction, and sender names, which are frequently (though not always) African or African inspired. Examples of senders and subject lines include those in the list below. You should note, however, that these examples are merely a few of the many thousands of variations of names, subject lines, or stories used in these scams.

Sender	Subject Line
usman bello	URGENT REPLY NEEDED
Charles Conneh	Re: Pleased to meet you!
Miss Kate Kasaka	Miss Kate Kasaka
Mr.Adnan A.K.Ismail	Cooperation
MR. Michael Okpala.	Good dey from MR. Michael Okpala.

A 419 advance fee fraud begins with an email that looks like this:

> Date: Wednesday, August 24, 2005 5:55 PM -0700
> From: "Mr. Henry Bassey Udoma" <henrybassey_udoma@example.com.ar>
> To: mrtarget@example.com
> Subject: From: Henry (Regarding Dr. H. Paul Jacobi)
>
> From: Henry (Regarding Dr. H. Paul Jacobi)
>
> Hello,
>
> I am sending you this private email to make a passionate appeal to you for assistance. Kindly accept my apology for contacting you this way and forgive me if this is not acceptable to you. My name is Henry Bassey Udoma; I am an auditor at one of the Nigerian Banks. On Tuesday, 19 January, 1999, one Dr. H. Paul Jacobi a foreigner, made a numbered time (Fixed) Deposit, valued at £10,550,000.00 (Ten Million, Five Hundred and Fifty Thousand Pounds) for twelve calendar months in my Bank Branch.
>
> Upon Maturity, we sent a routine notification to his forwarding address but got no reply. After a month, we sent a reminder and finally we discovered from his company that Dr. Paul A. Jacobi was aboard the Egypt Air Flight 990, which crashed into the Atlantic Ocean on October 31, 1999. After further investigation, it was discovered that he died without making a WILL and all attempts to trace his next of kin proved abortive….

These schemes work by getting the victim to take the initial bait, then slowly convincing him or her of the legitimacy of the plot through a series of forged documents, carefully crafted communications, and even visits by the victim to the country of origin for meetings with bogus "officials" in phony "government offices." At key junctures in the scam, the perpetrators will ask the victim to advance them money to pay bogus fees or bribes. Additionally, they may extract what amounts to an extortion payment by threatening to cut the victim out of the plot. Once the perpetrators believe they've gotten all they could from the victim, they cut off communication and vanish.

In short, if you discover an email in your inbox proposing a complicated arrangement to secure and split funds in a foreign land, you can safely assume someone is trying to ensnare you in a 419 scam.

Social Engineering/Phishing Email

Social engineering is a strategy for obtaining information people wouldn't normally divulge, or prompting an action people normally wouldn't perform, by preying on their natural curiosity and/or willingness to trust. Perpetrators of scams and other malicious individuals combine social engineering with email in a number of ways.

Phishing Email

Phishing emails are crafted to look as if they've been sent from a legitimate organization. These emails attempt to fool you into visiting a bogus web site to either download malware (viruses and other software intended to compromise your computer) or reveal sensitive personal information. The perpetrators of phishing scams carefully craft the bogus web site to look like the real thing.

For instance, an email can be crafted to look like it is from a major bank. It might have an alarming subject line, such as “Problem with Your Account.” The body of the message will claim there is a problem with your bank account and that, in order to validate your account, you must click a link included in the email and complete an online form.

The email is sent as spam to tens of thousands of recipients. Some, perhaps many, recipients are customers of the institution. Believing the email to be real, some of these recipients will click the link in the email without noticing that it takes them to a web address that only resembles the address of the real institution. If the email is sent and viewed as HTML, the visible link may be the URL of the institution, but the actual link information coded in the HTML will take the user to the bogus site. For example

visible link:	http://www.yourbank.com/accounts/
actual link to bogus site:	http://itcare.co.kr/data/yourbank/index.html

The bogus site will look astonishingly like the real thing, and will present an online form asking for information like your account number, your address, your online banking username and password—all the information an attacker needs to steal your identity and raid your bank account.

What to Look For

Bogus communications purporting to be from banks, credit card companies, and other financial institutions have been widely employed in phishing scams, as have emails from online auction and retail services. Carefully examine any email from your banks and other financial institutions. Most have instituted policies against asking for personal or account information in emails, so you should regard any email making such a request with extreme skepticism.

Phishing emails have also been disguised in a number of other ways. Some of the most common phishing emails include the following:

- fake communications from online payment and auction services, or from internet service providers – These emails claim there is a “problem” with your account and request that you access a (bogus) web page to provide personal and account information.
- fake accusation of violating Patriot Act – This email purports to be from the Federal Deposit Insurance Corporation (FDIC). It says that the FDIC is refusing to ensure your account because of “suspected violations of the USA Patriot Act.” It requests you provide information through an online form to “verify your identity.” It’s really an attempt to *steal* your identity.
- fake communications from an IT Department – These emails will attempt to ferret passwords and other information phishers can use to penetrate your organization’s networks and computers.
- low-tech versions of any of the above asking you to *fax* back information on a printed form you can download from a (bogus) web site.

The Anti-Phishing Working Group maintains a helpful phishing archive. The archive catalogues reported phishing scams and presents not only the content of the phishing email, but also screen captures of the bogus web sites and URLs used in the scams. A review of several of the phishing scams catalogued in the archive can provide you insight into how these scams work and arm you with the information you need to avoid falling for them. You can find the Anti-Phishing Working Groups phishing archive at the following address:

http://www.antiphishing.org/phishing_archive.html

Trojan Horse Email

Trojan horse email offers the promise of something you might be interested in—an attachment containing a joke, a photograph, or a patch for a software vulnerability. When opened, however, the attachment may do any or all of the following:

- create a security vulnerability on your computer
- open a secret "backdoor" to allow an attacker future illicit access to your computer
- install software that logs your keystrokes and sends the logs to an attacker, allowing the attacker to ferret out your passwords and other important information
- install software that monitors your online transactions and activities
- provide an attacker access to your files
- turn your computer into a "bot" an attacker can use to send spam, launch denial-of-service attacks, or spread the virus to other computers

What to Look For

Trojan horse emails have come in a variety of packages over the years. One of the most notorious was the "Love Bug" virus, attached to an email with the subject line "I Love You" and which asked the recipient to view the attached "love letter." Other Trojan horse emails have included the following:

- email posing as virtual postcard
- email masquerading as security bulletin from a software vendor requesting the recipient apply an attached "patch"
- email with the subject line "funny" encouraging the recipient to view the attached "joke"
- email claiming to be from an anti-virus vendor encouraging the recipient to install the attached "virus sweeper" free of charge

Virus-Generated Email

Note that, in some cases, a familiar "from" address does not ensure safety: Many viruses spread by first searching for all email addresses on an infected computer and then sending themselves to

these addresses. So, if your friend's computer has become infected with such a virus, you could receive an email that may, in fact, come from your friend's computer but which was not actually authored by your friend. If you have any doubts, verify the message with the person you believe to be the sender before opening any email attachment.

What You Can Do to Avoid Becoming a Victim

Filter Spam

Because most email scams begin with unsolicited commercial email, you should take measures to prevent spam from getting into your mailbox. Most email applications and web mail services include spam-filtering features, or ways in which you can configure your email applications to filter spam. Consult the help file for your email application or service to find out what you must do to filter spam.

You may not be able to eliminate *all* spam, but filtering will keep a great deal of it from reaching your mailbox. You should be aware that spammers monitor spam filtering tools and software and take measures to elude them. For instance, spammers may use subtle spelling mistakes to subvert spam filters, changing "Potency Pills" to "Potençy Pills."

Regard Unsolicited Email with Suspicion

Don't automatically trust any email sent to you by an unknown individual or organization. Never open an attachment to unsolicited email. Most importantly, never click on a link sent to you in an email. Cleverly crafted links can take you to forged web sites set up to trick you into divulging private information or downloading viruses, spyware, and other malicious software.

Spammers may also use a technique in which they send unique links in each individual spam email. Victim 1 may receive an email with the link <http://dfnasdunf.example.org/>, and victim 2 may receive the same spam email with the link <http://vnbnnasd.exaple.org/>. By watching which links are requested on their web servers, spammers can figure out which email addresses are valid and more precisely target victims for repeat spam attempts.

Remember that even email sent from a familiar address may create problems: Many viruses spread themselves by scanning the victim computer for email addresses and sending themselves to these addresses in the guise of an email from the owner of the infected computer.

Treat Email Attachments with Caution

Email attachments are commonly used by online scammers to sneak a virus onto your computer. These viruses can help the scammer steal important information from your computer, compromise your computer so that it is open to further attack and abuse, and convert your computer into a 'bot' for use in denial-of-service attacks and other online crimes. As noted above,

a familiar “from” address is no guarantee of safety because some viruses spread by first searching for all email addresses on an infected computer and then sending itself to these addresses. It could be your friend’s computer is infected with just such a virus.

Use Common Sense

When email arrives in your mailbox promising you big money for little effort, accusing you of violating the Patriot Act, or inviting you to join a plot to grab unclaimed funds involving persons you don’t know in a country on the other side of the world, take a moment to consider the likelihood that the email is legitimate.

Install Anti-virus Software and Keep it Up to Date

If you haven’t done so by now, you should install anti-virus software on your computer. If possible, you should install an anti-virus program that has an automatic update feature. This will help ensure you always have the most up-to-date protection possible against viruses. In addition, you should make sure the anti-virus software you choose includes an email scanning feature. This will help keep your computer free of email-born viruses.

Install a Personal Firewall and Keep it Up to Date

A firewall will not prevent scam email from making its way into your mailbox. However, it may help protect you should you inadvertently open a virus-bearing attachment or otherwise introduce malware to your computer by following the instructions in the email. The firewall, among other things, will help prevent outbound traffic from your computer to the attacker. When your personal firewall detects suspicious outbound communications from your computer, it could be a sign you have inadvertently installed malicious programs on your computer.

Learn the Email Policies of the Organizations You Do Business With

Most organizations doing business online now have clear policies about how they communicate with their customers in email. Many, for instance, will not ask you to provide account or personal information via email. Understanding the policies of the organizations you do business with can help you spot and avoid phishing and other scams. Do note, however, that it’s never a good idea to send sensitive information via unencrypted email.

Configure Your Email Client for Security

There are a number of ways you can configure your email client to make you less susceptible to email scams. For instance, configuring your email program to view email as “text only” will help protect you from scams that misuse HTML in email.

Further Reading

Anti-Phishing Working Group Phishing Archive
http://www.antiphishing.org/phishing_archive.html

FTC Consumer Alert: 12 Scams Most Likely To Arrive Via Bulk Email
http://www.ftc.gov/bcp/conline/pubs/alerts/doznalrt.htm

FTC Consumer Alert: How Not to Get Hooked by a 'Phishing' Scam
http://www.ftc.gov/bcp/conline/pubs/alerts/phishingalrt.htm4

Microsoft: How to Tell If a Microsoft Security Message is Genuine
http://www.microsoft.com/security/incident/authenticate_mail.mspx

United States Secret Service Advance Fee Fraud Advisory
http://www.secretservice.gov/alert419.shtml

US-CERT Cyber Security Tip ST04-007: Reducing Spam
http://www.us-cert.gov/cas/tips/ST04-007.html

US-CERT Cyber Security Tip ST04-010: Using Caution with Email Attachments
http://www.us-cert.gov/cas/tips/ST04-010.html

US-CERT Technical Cyber Security Alert TA05-189A: Targeted Trojan Email Attacks
http://www.us-cert.gov/cas/techalerts/TA05-189A.html

Produced 2005 by US-CERT, a government organization.