



Useful Information for Online Security

Contents compiled from Online Security Teams, aka White Hat Hackers (Hacking for the good to find Computer Vulnerabilities) and other Online Programming Security Firms.

- [10 Tips for a Total Online Security](#)
- [What is Phishing?](#)
- [How to Identify and Avoid Phishing Scams](#)
- [How Antivirus Software Works](#)
- [How Firewalls Work](#)
- [10 Tips to Avoid Getting Adware](#)
- [Beware of Common Internet Scams and Frauds](#)
- [How to Protect an Email Account from Being Hacked](#)
- [Conclusion](#)

10 Tips for a Total Online Security

With the sudden rise in the Internet usage across the globe over the past few years, there has also been a rise in the amount of online scams and frauds. Today most of the Internet users are unaware of the most prevailing online threats which pose a real challenge for their safe Internet usage. As a result, Online Security has become a questionable factor for the most Internet users. However it is still possible to effectively combat online insecurity provided that the users are well aware of the common scams and frauds and know how to protect themselves. A study shows that over 91% of the Internet users are unaware of the online scams and are worried about their security. Well if you are one among those 91% then here is a list of 10 tips to ensure your total online security.

1. Always install a good antivirus software and keep it up-to-date. Also install a good anti-spyware to keep your PC away from spywares. [Click Here](#) for a list of recommended anti-spyware softwares.
2. Always visit known and trusted websites. If you are about to visit an unknown website, ensure that you do not click on suspectable links and banners.
3. Perform a virus scan on the files/email attachments that you download before executing them.
4. Regularly Update your operating system and browser software. For a better security it is recommended that you surf the Internet through the latest version of your browser program.

5. Never share your password (email, bank logins etc.) with any one for any reason. Choose a strong password (A blend of alphanumeric+special symbols) and change it regularly, eg. every 3 months. Avoid using easy-to-guess passwords. (ex. pet's name or kid's name)

6. Always type the URL of the website in your browser's address bar to enter the login pages. For ex. To login to your Gmail account type <http://mail.google.com>

7. Before you enter your password on any login page, ensure that you see **https** instead of **http**. ex. <https://mail.google.com> instead of <http://mail.google.com>. HTTPS protocol implements SSL (Secure Sockets Layer) and provide better security than a normal HTTP. For more information on HTTPS and SSL see [Know More About Secure Sockets Layer \(SSL\)](#).

8. Beware of phishing emails! Do not respond to any email that request you to update your login details by clicking on a link in the body of the email. Such links can lead to Fake Login Pages (Spoofed Pages).

9. Always hit the logout button to close your login session rather than abruptly terminating the browser window. Also clear your web browser caches after every session to remove the temporary files stored in the memory and hard disk of your PC.

10. Avoid (Stop) using any public computers or computers in the Internet cafes to access any sensitive/confidential information. Also avoid such computers to login to your email/bank accounts. You cannot be sure if any spyware, keystroke-logger, password-sniffer and other malicious programs have not been installed on such a PC.

By following the above 10 tips your online security can be guaranteed upto 90%. I hope this will help my readers for keeping themselves safe from any of the online insecurities. Cheers! Pass your comments.

- [Back to Top](#) -

What is Phishing?

Phishing is an attempt to criminally and fraudulently acquire sensitive information, such as usernames, passwords and credit card details, by appearing as a trustworthy entity in an electronic communication. eBay, PayPal and other online banks are common targets.

Phishing is typically carried out by email or instant messaging and often directs users to enter details at a website, although phone contact has also been used.

Phishing is an example of social engineering techniques used to fool users. Attempts to deal with the growing number of reported phishing incidents include legislation, user training, public awareness, and technical measures.

Recent phishing attempts have targeted the customers of banks and online payment services. Social networking sites such as Orkut are also a target of phishing.

Spoofed/Fraudulent e-mails are the most widely used tools to carry out the phishing attack. In most cases we get a fake e-mail that appears to have come from a Trusted Website . Here the hacker may request us to verify username & password by replaying to a given email address.

TECHNIQUES BEHIND PHISHING ATTACK

1. Link Manipulation

Most methods of phishing use some form of technical deception designed to make a link in an email appear to belong to some trusted organization or spoofed organization. Misspelled URLs or the use of subdomains are common tricks used by phishers, such as this example URL

www.micosoft.com

www.mircosoft.com

www.verify-microsoft.com

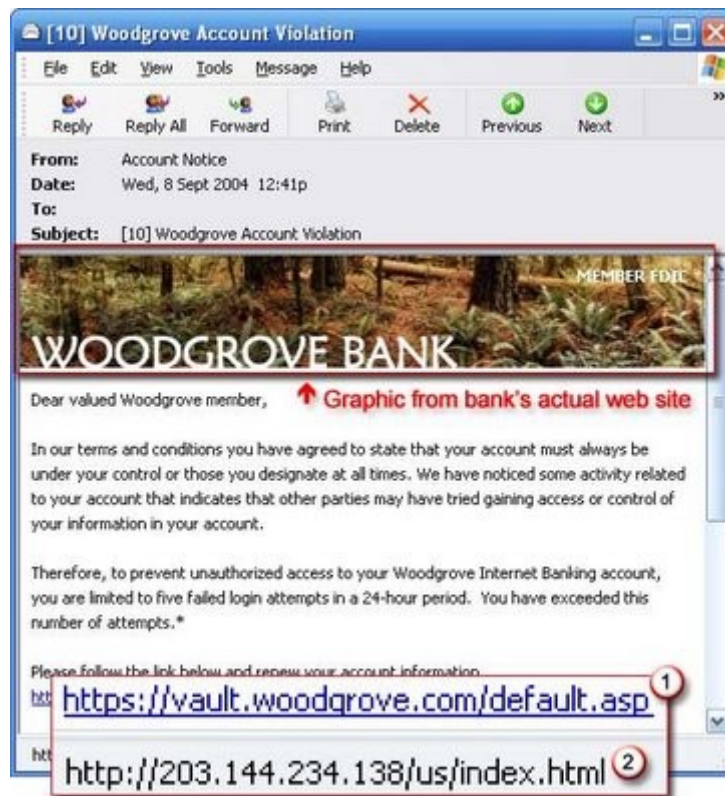
instead of www.microsoft.com

2. Filter Evasion

Phishers have used images instead of text to make it harder for anti-phishing filters to detect text commonly used in phishing emails. This is the reason [Gmail](#) or [Yahoo](#) will disable the images by default for incoming mails.

How does a phishing attack/scam look like?

As scam artists become more sophisticated, so do their phishing e-mail messages and pop-up windows. They often include official-looking logos from real organizations and other identifying information taken directly from legitimate Web sites. Here is an example of how the phishing scam email looks like



Example of a phishing e-mail message, including a deceptive URL address linking to a scam Web site.

To make these phishing e-mail messages look even more legitimate, the scam artists may place a link in them that appears to go to the legitimate Web site (1), but it actually takes you to a phishing site (2) or possibly a pop-up window that looks exactly like the official site.

These copycat sites are also called “spoofed” Web sites. Once you’re at one of these spoofed sites, you may send personal information to the hackers.

How to identify a fraudulent e-mail?

Here are a few phrases to look for if you think an e-mail message is a phishing scam.

“Verify your account.”

Legitimate sites will never ask you to send passwords, login names, Social Security numbers, or any other personal information through e-mail.

“If you don’t respond within 48 hours, your account will be closed.”

These messages convey a sense of urgency so that you’ll respond immediately without thinking.

“Dear Valued Customer.”

Phishing e-mail messages are usually sent out in bulk and *often do not contain your first or last name.*

“Click the link below to gain access to your account.”

HTML-formatted messages can contain links or forms that you can fill out just as you’d fill out a form on a Web site. The links that you are urged to click may contain all or part of a real company’s name and are usually “masked,” meaning that the link you see does not take you to that address but somewhere different, usually a scam Web site.

Notice in the following example that resting the mouse pointer on the link reveals the real Web address, as shown in the box with the yellow background. The string of cryptic numbers looks nothing like the company's Web address, which is a suspicious sign.



So the Bottom line to defend from phishing attack is

1. Never assume that an email is valid based on the sender's email address.
2. A trusted bank/organization such as paypal will never ask you for your full name and password in a PayPal email.
3. An email from trusted organization will never contain attachments or software.
4. Clicking on a link in an email is the most insecure way to get to your account.

- [Back to Top](#) -

How to Identify and Avoid Phishing Scams

Phishing is a form of social engineering technique used by hackers to gather sensitive information such as usernames, passwords and credit card details by posing as a trustworthy person/organization. Since most online users are unaware of the techniques used in carrying out a phishing attack, they often fall victims and hence, phishing can be very effective.


With the dramatic increase in the number of phishing scams in the recent years, there has also been a steady rise in the number of people being victimized. Lack of awareness among the people is the prime reason behind such attacks. This article will try to create awareness and educate the users about such online scams and frauds.

Phishing scams usually sends an email message to users requesting for their personal information, or redirects them to a website where they are required to enter their personal information. Here are some of the tips that can be used to identify various phishing techniques and stay away from it.

Identifying a Phishing Scam

1. Beware of emails that demand for an urgent response from your side. Some of the examples are:
 - You may receive an email which appears to have come from your bank or financial organization stating that “your bank account is limited due to an unauthorized activity. Please *verify your account* asap so as to avoid permanent suspension”. In most cases, you are requested to follow a link (URL) that takes you to spoofed webpage (similar to your bank website) and enter your login details over there.
 - In some cases, phishing emails may ask you to make a phone call. There may be a person or an audio response waiting on the other side of the phone to take away your credit cards details, account number, social security number or other valuable data.
2. Phishing emails are generally not personalized. Since they target a large number of online users, they usually use generalized texts like “Dear valued customer”, “Dear Paypal user” etc. to address you. However, some phishing emails can be an exception to this rule.
3. When you click on the links contained in a phishing email, you will most likely be taken to a spoofed webpage with official logos and information that looks exactly same as that of the original webpages of your bank or financial organization. Pay attention to the URL of a website before you enter any of your personal information over there. Even though malicious websites look identical to the legitimate site, it often uses a different domain or variation in the spelling. For example, instead of [paypal.com](https://www.paypal.com), a phishing website may use different addresses such as:
 - [papyal.com](https://www.papyal.com)
 - [paypal.org](https://www.paypal.org)
 - [verify-paypal.com](https://www.verify-paypal.com)
 - [xyz.com/paypal/verify-account/](https://www.xyz.com/paypal/verify-account/)

Tips to Avoid Being a Victim of Phishing

1. Do not respond to suspicious emails that ask you to give your personal information. If you are unsure whether an email request is legitimate, verify the same by calling the respective bank/company. Always use the telephone numbers printed on your bank records or statements and not those mentioned in the suspicious email.
2. Don't use the links in an email, instant messenger or chat conversation to enter a website. Instead, always type the URL of the website on your browser's address bar to get into a website.
3. Legitimate websites always use a secure connection (https://) on those pages which are intended to gather sensitive data such as usernames and passwords, account numbers or credit card details. You will see a lock icon  in your browser's address bar which indicates a secure connection. On some websites like paypal.com which uses an extended validation certificate, the address bar turns GREEN as shown below.



In most cases, unlike a legitimate website, a phishing website or a spoofed webpage will not use a secure connection and does not show up the lock icon. So, absence of such security features can be a clear indication of phishing attack. Always double-check the security features of the webpage before entering any of your personal information.

4. Always use a good antivirus software, firewall and email filters to filter the unwanted traffic. Also ensure that your browser is up-to-date with the necessary patches being applied.
5. Report a “phishing attack” or “spoofed emails” to the following groups so as to stop such attacks from spreading all over the Internet:

You can directly send an email to spoof@paypal.com or spam@uce.gov or reportphishing@antiphishing.org reporting an attack. You can also notify the Internet Crime Complaint Center of the FBI by filing a complaint on their website: www.ic3.gov.

- [Back to Top](#) -

How Antivirus Software Works

Due to ever increasing threat from virus and other malicious programs, almost every computer today comes with a pre-installed antivirus software on it. In fact, an antivirus has become one of the most essential software package for every computer. Even though every one of us have an antivirus software installed on our computers, only a few really bother to understand how it actually works! Well if you are one among those few who would really bother to understand how an antivirus works, then this article is for you.

How Antivirus Works

An antivirus software typically uses a variety of strategies in detecting and removing viruses, worms and other malware programs. The following are the two most widely employed identification methods:

1. Signature-based detection (Dictionary approach)

This is the most commonly employed method which involves searching for known patterns of virus within a given file. Every antivirus software will have a dictionary of sample malware codes called *signatures* in it's database. Whenever a file is examined, the antivirus refers to the dictionary of sample codes present within it's database and compares the same with the current file. If the piece of code within the file matches with the one in it's dictionary then it is flagged and proper action is taken immediately so as to stop the virus from further replicating. The antivirus may choose to repair the file, quarantine or delete it permanently based on it's potential risk.

As new viruses and malwares are created and released every day, this method of detection cannot defend against new malwares unless their samples are collected and signatures are released by the antivirus software company. Some companies may also encourage the users to upload new viruses or variants, so that the virus can be analyzed and the signature can be added to the dictionary.

Signature based detection can be very effective, but requires frequent updates of the virus signature dictionary. Hence the users must update their antivirus software on a regular basis so as to defend against new threats that are released daily.

2. Heuristic-based detection (Suspicious behaviour approach)

Heuristic-based detection involves identifying *suspicious behaviour* from any given program which might indicate a potential risk. This approach is used by some of the sophisticated antivirus softwares to identify new malware and variants of known malware. Unlike the signature based approach, here the antivirus doesn't attempt to identify known viruses, but instead monitors the behavior of all programs.

For example, malicious behaviours like a program trying to write data to an executable program is flagged and the user is alerted about this action. This method of detection gives an additional level of security from unidentified threats.

File emulation: This is another type of *heuristic-based approach* where a given program is executed in a virtual environment and the actions performed by it are logged. Based on the actions logged, the antivirus software can determine if the program is malicious or not and carry out necessary actions in order to clean the infection.

Most commercial antivirus softwares use a combination of both signature-based and heuristic-based approaches to combat malware.

Issues of concern

Zero-day threats: A zero-day (zero-hour) threat or attack is where a malware tries to exploit computer application vulnerabilities that are yet unidentified by the antivirus software companies. These attacks are used to cause damage to the computer even before they are identified. Since patches are not yet released for these kind of new threats, they can easily manage to bypass the antivirus software and carry out malicious actions. However most of the threats are identified after a day or two of it's release, but damage caused by them before identification is quite inevitable.

Daily Updates: Since new viruses and threats are released everyday, it is most essential to update the antivirus software so as to keep the virus definitions up-to-date. Most softwares will have an auto-update feature so that the virus definitions are updated whenever the computer is connected to the Internet.

Effectiveness: Even though an antivirus software can catch almost every malware, it is still not 100% foolproof against all kinds of threats. As explained earlier, a zero-day threat can easily bypass the protective shield of the antivirus software. Also virus authors have tried to stay a step ahead by writing "[oligomorphic](#)", "[polymorphic](#)" and, more recently, "[metamorphic](#)" virus codes, which will encrypt parts of themselves or otherwise modify themselves as a method of disguise, so as to not match virus signatures in the dictionary.

Thus user education is as important as antivirus software; users must be trained to practice safe surfing habits such as downloading files only from trusted websites and not blindly executing a program that is unknown or obtained from an untrusted source. I hope this article will help you understand the working of an antivirus software.

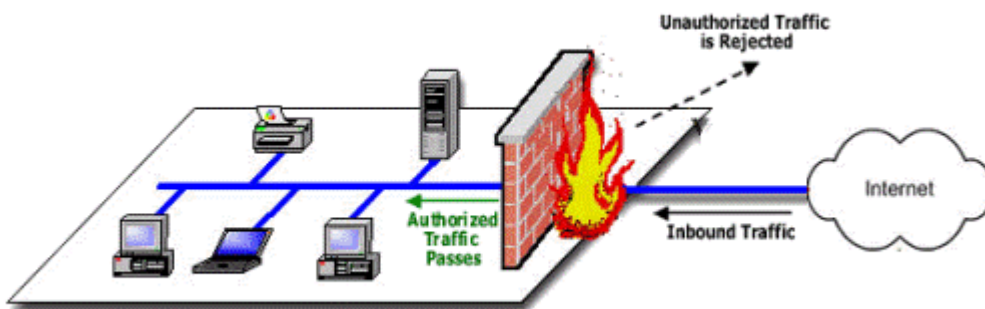
- [Back to Top](#) -

How Firewalls Work

If you have been using Internet on a regular basis or working in a large company and surf the Internet while you are at work, you must have surely come across the term firewall. You might have also heard of people saying “firewalls protect their computer from web attacks and hackers” or “a certain website has been blocked by firewall in their work place”. If you have ever wondered to know what exactly is this firewall and how it works, here we go. In this post I will try to explain “How firewalls work” in a layman’s terms.

How Firewalls Work

Firewalls are basically a barrier between your computer (or a network) and the Internet (outside world). A firewall can be simply compared to a security guard who stands at the entrance of your house and filters the visitors coming to your place. He may allow some visitors to enter while denying others whom he suspects of being intruders. Similarly a firewall is a software program or a hardware device that filters the information (packets) coming through the Internet to your personal computer or a computer network.



Firewalls may decide to allow or block network traffic between devices based on the rules that are pre-configured or set by the firewall administrator. Most personal firewalls such as Windows firewall operate on a set of pre-configured rules that are most suitable under normal circumstances so that the user need not worry much about configuring the firewall.

Personal firewalls are easy to install and use and hence preferred by end-users for use on their personal computers. However large networks and companies prefer those firewalls that have plenty of options to configure so as to meet their customized needs. For example, a company may set up different firewall rules for FTP servers, Telnet servers and Web servers. In addition the company can even control how the employees connect to the Internet by blocking access to certain websites or restricting the transfer of files to other networks. Thus in addition to security, a firewall can give the company a tremendous control over how people use the network.

Firewalls use one or more of the following methods to control the incoming and outgoing traffic in a network:

1. Packet Filtering: In this method packets (small chunks of data) are analyzed against a set of **filters**. Packet filters has a set of rules that come with accept and deny actions which are pre-configured or can be configured manually by the firewall administrator. If the packet manages to make it through these filters then it is allowed to reach the destination; otherwise it is discarded.

2. Stateful Inspection: This is a newer method that doesn’t analyze the contents of the packets. Instead it compares certain key aspects of each packet to a database of trusted source. Both incoming and outgoing packets are compared against this database and if the comparison yields a reasonable match, then the packets are allowed to travel further. Otherwise they are discarded.

Firewall Configuration

Firewalls can be configured by adding one or more filters based on several conditions as mentioned below:

1. IP addresses: In any case if an [IP address](#) outside the network is said to be unfavorable, then it is possible to set filter to block all the traffic to and from that IP address. For example, if a certain IP address is found to be making too many connections to a server, the administrator may decide to block traffic from this IP using the firewall.

2. Domain names: Since it is difficult to remember the IP addresses, it is an easier and smarter way to configure the firewalls by adding filters based on domain names. By setting up a domain filter, a company may decide to block all access to certain domain names, or may provide access only to a list of selected domain names.

3. Ports/Protocols: Every service running on a server is made available to the Internet using numbered ports, one for each service. In simple words, ports can be compared to virtual doors of the server through which services are made available. For example, if a server is running a Web (HTTP) service then it will be typically available on port 80. In order to avail this service, the client needs to connect to the server via port 80. Similarly different services such as Telnet (Port 23), FTP (port 21) and SMTP (port 25) services may be running on the server. If the services are intended for the public, they are usually kept open. Otherwise they are blocked using the firewall so as to prevent intruders from using the open ports for making unauthorized connections.

4. Specific words or phrases: A firewall can be configured to filter one or more specific words or phrases so that, both the incoming and outgoing packets are scanned for the words in the filter. For example, you may set up a firewall rule to filter any packet that contains an offensive term or a phrase that you may decide to block from entering or leaving your network.

Hardware vs. Software Firewall

Hardware firewalls provide higher level of security and hence preferred for servers where security has the top most priority whereas, the software firewalls are less expensive and are most preferred in home computers and laptops. Hardware firewalls usually come as an in-built unit of a router and provide maximum security as it filters each packet in the hardware level itself even before it manages to enter your computer. A good example is the Linksys Cable/DSL router.

Why Firewall?

Firewalls provide security over a number of online threats such as Remote login, Trojan backdoors, Session hijacking, DOS & DDOS attacks, viruses, cookie stealing and many more. The effectiveness of the security depends on the way you configure the firewall and how you set up the filter rules. However major threats such as DOS and DDOS attacks may sometimes manage to bypass the firewalls and do the damage to the server. Even though firewall is not a complete answer to online threats, it can most effectively handle the attacks and provide security to the computer up to the maximum possible extent.

10 Tips to Avoid Getting Adware

Adware, malware, spyware and viruses can bring your system to its knees. They are detrimental, lowering the performance of your computer. You might need to replace data. You might lose unique files. Keep the nasties away from your computer using these ten simple tips.

1. **Use Firefox:** Internet Explorer is the most popular browser on the market, controlling over 50% of the market share. The virus and adware creators specifically look for exploitable vulnerabilities within IE because they know that they will receive the best return on investment. Your switch to Firefox prevents some adware from infecting your machine.
2. **Scan your PC once a week:** Sometimes adware programmers take a sneaky approach. They will set up their programs to run quietly in the background to spy upon your activities. This once a week scan is necessary to remove any of those sneaky bugs.
3. **Download from known sites:** New sites for installing adware are popping up all the time. If you find something that you want to download, make sure that it is from a known site. A company like Amazon will not steer you wrong, but Bob's House of Wares might be a little less trustable. If you are not sure whether you can trust a site, perform a quick search.
4. **Install Adaware:** [Ad-Aware](#) is the most popular free adware removal program on the market. It detects, quarantines and removes adware. It searches for other programs which may have been installed, highlighting them in an easy to use interface. This program does not have an anti-virus attached.
5. **Do not click on unsolicited email:** You are constantly receiving offers to increase this or improve that through unsolicited email. Your curiosity may be killing you, but don't click on these emails. They accept your click as permission to install adware, spyware and malware on your PC.
6. **Install Antivirus software:** Installing two programs for virus and adware protection is a smart idea. It caters to the strengths of each program, increasing the overall strength of your antiadware and antiviral campaign. Some of the best antivirus software is free, providing real time protection. Programs to look at would be Avast Antivir and AVG.
7. **Don't install toolbars:** Even some reputable sites install custom toolbars. They slow your system down and collect information about your surfing habits. While a toolbar might offer some perks, it may also diminish your experience by dragging your system to a halt. Toolbars from less reputable places install adware and sometimes infect your system outright.
8. **Look at your task manager:** If anything seems out of place with your computer, take a look at your task manager. This tells you about all of the programs and processes which are running on your computer. Examine the processes tab for anything which you don't immediately recognize. Perform a web search for unfamiliar processes.
9. **Do not click on popups:** Clicking on a popup usually spells certain doom for your computer. It opens the door for the viruses and adware that want to infect your machine, telling these malicious applications to make themselves at home. Stay away from those constantly advertised screensavers and icons.
10. **Trust your gut:** If you don't feel right about a site, don't go there. If you are receiving warnings from the antivirus and antiadware programs which you've installed, don't go there. If you don't like the layout of a site, don't go there. Trust your instincts about sites.

With proper vigilance, you can keep aggravating adware, spyware and malware from your machine. Trust your instincts. Install [Ad-Aware](#) and an antivirus program. Play it safe. The care you spend in preventing adware from infecting your machine can save money and time.

Beware of Common Internet Scams and Frauds

The term **Internet Scam** or **Internet Fraud** refers to any type of fraud scheme that uses one or more online services to conduct fraudulent activities. Internet fraud can take place on computer programs such as chat rooms, e-mail, message boards, or Web sites. In this post I will discuss about some of the commonly conducted scams and frauds across the Internet.

1. Phishing Scam

This is one of the most commonly used scam to steal bank logins and other types of passwords on the Internet. **Phishing** is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication. Phishing is typically carried out by e-mail or instant messaging.

Example: You may receive an email which claims to have come from your bank/financial institution/online service provider that asks you to click a link and update your account information. When you click such a link it will take you to a fake page which exactly resembles the original ones. Here you'll be asked to enter your personal details such as username and password. Once you enter your personal details they will be stolen away. Such an email is more than likely the type of Internet scam known as "phishing". Phishing is said to be highly effective and has proved to have more success rate since most of the common people fail to identify the scam.

Most legitimate companies never request any kind of personal/sensitive information via email. So it is highly recommended that you **DO NOT** respond to such fraudulent emails.

2. Nigerian Scams

This type of scam involves sending emails (spam) to people in bulk seeking their help to access large amount of money that is held up in a foreign bank account. This email claims that in return for the help you'll be rewarded a percentage of the fund that involves in the transaction. Never respond to these emails since it's none other than a scam.

In case if you respond to these emails you will be asked to deposit a small amount of money (say 1-2% of the whole fund) as an insurance or as an advance payment for the initialization of deal. However once you deposit the amount to the scammer's account you'll not get any further response from them and you lose your money. In fact "The large amount of money" never exists and the whole story is a trap for innocent people who are likely to become victims. The scammers use a variety of stories to explain why they need your help to access the funds. The following are some of the examples of them.

Examples:

- They may claim that political climate or legal issues preclude them from accessing funds in a foreign bank account
- They may claim that the person is a minor and hence needs your help to access the funds
- They may claim that your last name is the same as that of the deceased person who owned the account and suggest that you act as the Next of Kin of this person in order to gain access to the funds

3. Lottery Scams

This type of scam is similar to the one discussed above. In this type you may receive an email saying that you have won a large sum of money in online lottery scheme (ex. UK Lottery) even though you have not participated in any such schemes. The message claims that your email ID was selected randomly from a large pool of IDs. When you respond to such emails they initially ask for your complete name and address so that they can mail the cheque across to you. After getting those details they may also send you an image of the cheque drawn in your name and address so as to confirm the deal. But in order to mail this cheque they demand a small amount of money as insurance/shipping charge/tax in return. However if you send the amount in hope to receive the cheque all you get is nothing. You're just trapped in a wonderful scam scheme. That's it.

4. Other General Scams and Frauds

The following are some of the other types of scams that you should be aware of.

In general, be aware of unsolicited emails that:

1. Promise you money, jobs or prizes
2. Ask you to provide sensitive personal information
3. Ask you to follow a link to a website and log on to an account.
4. Propose lucrative business deals

However it may seem to be a difficult task for novice Internet users to identify such online scams. Here are some of the common signs of such scam emails. By knowing them it may help you to stay away.

- All these scam emails never address you by your name. In turn they commonly address you something like "Dear User" or "Dear Customer" etc. This is a clear indication that the email is a fraudulent one
- When you observe the email header you may notice in the "TO:" Field that, the same email is forwarded to a large group of people or the "TO:" field appears blank. So this confirms that the email was not intended particularly for you. It was forwarded for a large group of people and you are one among them

- [Back to Top](#) -

How to Protect an Email Account from being Hacked

Today in this post I'll teach you how to protect your email account from being hacked. Nowadays I get a lot of emails where most of the people say "My Email account is hacked please help...". Now one question which arises in our mind is: "Is it so easy to **hack an email account**? **OR** Is it so difficult to protect an email account from being hacked?". The single answer to these two questions is "Absolutely NOT!". It is neither easy to hack an email nor difficult to protect an email account from being hacked.

If this is the case, then what is the reason for many people to lose their accounts?

The answer is very simple. They don't know how to protect themselves from being hacked! In fact most of the people who lose their email accounts are not the victims of hacking but the victims of **Trapping**. They lose their passwords not because they are hacked by some expert hackers but they are fooled to such an extent that they themselves give away their password.

Are you confused? If so continue reading and you'll come to know...

Now I'll mention some of the most commonly used online scams which fool people and make them lose their passwords. I'll also mention how to protect your email account from these scams.

1. WEBSITE SPOOFING

Website spoofing is the act of creating a website, with the intention of misleading the readers. The website will be created by a different person or organisation (Other than the original) especially for the purposes of cheating. Normally, the website will adopt the design of the target website and sometimes has a similar URL.

For example a Spoofed Website of **Yahoo.com** appears exactly same as **Yahoo Website**. So most of the people believe that it is the original site and lose their passwords. The main intention of spoofed websites is to fool users and take away their passwords. For this, the spoofed sites offer **fake login pages**. These **fake login pages** resemble the original login pages of sites like Yahoo, Gmail, Orkut etc. Since it resembles the original login page people believe that it is true and give away their **username and passwords** by trying to login to their accounts.

Solution:

- Never try to login/access your email account from the sites other than the original site.
- Always type the URL of the site in the address bar to get into the site. Never click on the hyperlink to enter the site.

2. BY USING KEYLOGGERS

The other commonly used method to steal password is by using a **Keylogger**. A Keylogger is nothing but a spyware. The detailed description of keylogger and its usage is discussed in the post **Hacking an email account**. If you read this post you'll come to know that it is too easy to steal the password using a keylogger program. If you just access your email account from a computer installed with keylogger, you definitely lose your password. This is because the keylogger records each and every keystroke that you type.

Solution:

Protecting yourselves from a keylogger scam is very easy. Just install a good anti-spyware program and update it regularly. This keeps your PC secure from a keylogger. Also there is a program called [Anti-keylogger](#) which is specially designed to detect and remove keyloggers. You can use this program to detect some stealth keyloggers which remain undetected by many anti-spyware programs.

3. ACCESSING YOUR EMAIL ACCOUNT FROM CYBER CAFES

Do you access your email from cyber cafes? Then definitely you are under the risk of losing your password. In fact many people lose their email account in cyber cafes. For the owner of the cyber cafe it's just a cakewalk to steal your password. For this he just needs to install a keylogger on his computers. So when you login to your email account from this PC, you give away your password to the cafe owner. Also there are many Remote Administration Tools (RATs) which can be used to monitor your browsing activities in real time.

This doesn't mean that you should never use cyber cafes for browsing the internet. I know, not all the cyber cafe owners will be so wicked but it is recommended not to use cafes for accessing confidential information. If it comes to the matter of security never trust anyone, not even your friend. I always use my own PC to login to my accounts to ensure safety.

- [Back to Top](#) -

Conclusion

Hope this helps inform you about the simple measures that can be taken to improve your Online and Personal protection. This edition hasn't touched some other simple fixes for Software Configurations, but will be in the next file full of random knowledge in my head full of Online Security trinkets.

REMEMBER THE ABOVE REFERENCE ABOUT LOGGING INTO PAGES WITH **HTTPS://** AND NOT **HTTP://** FOR SECURITY. ESPECIALLY FOR FACEBOOK'S HOMEPAGE WITH THE LOGIN AT THE TOP. **DO NOT PUT ANYTHING** IN EITHER FIELD AND JUST HIT "LOGIN" WHICH WILL ERROR AND TAKE YOU TO A **HTTPS://** LOGIN PAGE.

Thank you,

Josh Rhoton
TCOB Web Designs LLC
www.tcobwebdesigns.com
971-225-5429



TCOB WEB DESIGNS LLC