

TOP 25 EMAIL SECURITY ISSUES



In this article we focus on 25 of the most common and easy to fix mistakes that people make when it comes to email security. We've designed this article with the new internet user in mind, so if you're an email expert, you may want to pass this along to your novice friends.

1. Using just one email account.

Individuals new to email often think about their email account like they do their home address, you only have one home address, so you should only have one email. Instead, you should think about your email address like you do your keys; while it may be OK to use the same key for your front and your back door, having a single key open everything is both impractical and unsafe.

A good rule of thumb for the average email user is to keep a minimum of three email accounts. Your work account should be used exclusively for work-related conversations. Your second email account should be used for personal conversations and contacts, and your third email account should be used as a general catch-all for all hazardous behavior. That means that you should always sign up for newsletters and contests only through your third email account. Similarly, if you have to post your email account online, such as for your personal blog, you should only use your third email account (and post a web friendly form of it at that).

While your first and second email accounts can be paid or freebie, your third 'catch-all' account should always be a freebie account such as those offered by Gmail or Yahoo!. You should plan on having to dump and change out this account every six months, as the catch-all account will eventually become spammed when a newsletter manager decides to sell your name or a spammer steals your email address off a Web site.

2. Holding onto spammed-out accounts too long.

It is simply a fact of life that email accounts will accumulate spam over time. This is especially true of the account you use to sign up for newsletters and that you post online (which as stated above should not be your main email account). When this happens, it is best to simply dump the email account and start afresh. Unfortunately, however, many new email users get very attached to their email accounts and instead just wade through dozens of pieces of spam every day. To avoid the problem, prepare yourself mentally ahead of time for the idea that you will have to dump your 'catch all' account every six months.

3. Not closing the browser after logging out.

When you are checking your email at a library or cybercafé you not only need to log out of your email when you are done, but you also need to make sure to close the browser window completely. Some email services display your username (but not your password) even after you have logged out. While the service does this for your convenience, it compromises your email security.

4. Forgetting to delete browser cache, history and passwords.

After using a public terminal, it is important that you remember to delete the browser cache, history, and passwords. Most browsers automatically keep track of all the web pages that you have visited, and some keep track of any passwords and personal information that you enter in order to help you fill out similar forms in the future.

If this information falls into the wrong hands, it can lead to identity theft and stolen bank and email information. Because the stakes are so high, it is important that new internet users be aware of how to clear a public computers browser cache so that they can delete private information before lurking hackers can get a hold of it.

TOP 25 EMAIL SECURITY ISSUES



Future - Now

For those of you using Mozilla's Firefox, simply press Ctrl+Shift+Del. Opera users need go to Tools>>Delete Private Data. And users of Microsoft's Internet Explorer need to go to Tools>>Internet Options then click the 'Clear History', 'Delete Cookies', and 'Delete Files' buttons.

5. Using unsecure email accounts to send and receive sensitive corporate information.

Large corporations invest huge amounts of money to ensure that their computer networks and email remain secure. Despite their efforts, careless employees using personal email accounts to conduct company business and pass along sensitive data can undermine the security measures in place. So make sure that you don't risk your company's security, and your job, by transmitting sensitive company data via your own personal computer or email address.

6. Forgetting the telephone option

One of the most important lessons about email security is that no matter how many steps you take to secure your email, it will never be foolproof. This is never truer than when using a public computer. So unless you need a written record of something or are communicating across the globe, consider whether a simple phone call rather than an email is a better option. While a phone conversation may require a few extra minutes, when compared with accessing email through a public computer, a phone call is a far more secure option and it does not leave a paper trail.

Emailing the right people

7. Not using the Blind Carbon Copy (BCC) option.

When you put a person's email addresses in the BCC: rather than the CC: window, none of the recipients can see the addresses of the other email recipients.

New email users often rely too much on the TO: because it is the default way of sending emails. That is fine as long as you are writing to just one person or a few family members. But if you are sending mail out to a diverse group of people, confusing BCC: and CC: raises some serious privacy and security concerns. It takes just one spammer to get a hold of the email and immediately everyone on your email list gets spammed.

Even if the honesty of the group isn't in question, many email programs are setup to automatically add to the address books any incoming email addresses. That means that some people in the group will inadvertently have added the entire list to their address book, and as a result, if one of their computers is infected with "Zombie" malware and silently sends out spam emails, you will have just caused the entire list to get spammed.

8. Being trigger happy with the "Reply All" button.

Sometimes the mistake isn't in deciding between CC: and BCC: but between hitting Reply All instead of Reply. When you hit Reply All, your email message is sent to everyone included on the original email, and if you didn't intend to include them, the information can be disastrous from both a security and personal humiliation perspective:

Example 1: "A very successful salesman at our networking company had a large email address book filled with his best customers, including some very important and conservative government contacts. With a single click, he accidentally sent a file chock-full of his favorite pornographic cartoons and jokes to everyone on his special customer list. His subject line: 'Special deals for my best customers!' Needless to say, he's cutting deals for another company these days."

TOP 25 EMAIL SECURITY ISSUES



Future - Now

Example 2: "A woman was in torment over a busted romance. She wrote a lengthy, detailed message to a girlfriend, adding that her ex-boyfriend preferred men to women. But instead of hitting Reply to a previous message from her girlfriend, she hit Reply All. Her secret was sent to dozens of people she didn't even know (including me), plus the aforementioned ex and his new boyfriend. As if that weren't bad enough, she did this two more times in quick succession!"

9. Spamming as a result of forwarding email.

Forwarding emails can be a great way to quickly bring someone up to speed on a subject without having to write up a summary email, but if you aren't careful, forwarding emails can create a significant security threat for yourself and the earlier recipients of the email. As an email is forwarded, the recipients of the mail (until that point in time) are automatically listed in the body of the email. As the chain keeps moving forward, more and more recipient ids are placed on the list.

Unfortunately, if a spammer or someone just looking to make a quick buck gets a hold of the email, they can then sell the entire list of email ids and then everyone will start to get spammed. It only takes a few seconds to delete all the previous recipient ids before forwarding a piece of mail, and it can avoid the terrible situation of you being the cause of all your friends or coworkers getting spammed.

Making backups and keeping records

10. Failing to back up emails.

Emails are not just for idle chatting, but can also be used to make legally binding contracts, major financial decisions, and conduct professional meetings. Just as you would keep a hard copy of other important business and personal documents, it is important that you regularly back up your email to preserve a record if your email client crashes and loses data (It happened to Gmail as recently as December 2006).

Thankfully, most email providers make it rather simple to back up your email by allowing you to export emails to a particular folder and then just creating a copy of the folder and storing it onto a writeable CD, DVD, removable disk, or any other type of media. If that simple exporting process sounds too complicated, you can just buy automated backup software that will take care of the whole thing for you. Whether you purchase the software or decide to back up manually, it is important that you make and follow a regular backup schedule, as this is the sort of thing that new email users tend to just put off. The frequency of backups necessary for you will of course depend on your email usage, but under no circumstances should it be done less frequently than every 3 months.

11. Mobile access: Presuming a backup exists.

Mobile email access, such as through BlackBerry, has revolutionized the way we think about email; no longer is it tied to a PC, but rather it can be checked on-the-go anywhere. Most new BlackBerry users simply assume that a copy of the emails they check and delete off the BlackBerry will still be available on their home or office computer.

It is important to keep in mind, however, that some email servers and client software download emails to the Blackberry device and then delete them from the server. Thus, for some mobile email access devices, if you delete it from the device, you have deleted it from your Inbox.

Just be aware of the default settings of your email client and make sure that if you want a copy of the email retained, you have adjusted the email client's settings to make it happen. And preferably make sure of this *before* you decide to delete that important email.

TOP 25 EMAIL SECURITY ISSUES



12. Thinking that an erased email is gone forever.

We've all sent an embarrassing or unfortunate email and sighed relief when it was finally deleted, thinking the whole episode was behind us. Think again. Just because you delete an email message from your inbox and the sender deletes it from their 'Sent' inbox, does not mean that the email is lost forever. In fact, messages that are deleted often still exist in backup folders on remote servers for years, and can be retrieved by skilled professionals.

So start to think of what you write in an email as a permanent document. Be careful about what you put into writing, because it can come back to haunt you many years after you assumed it was gone forever.

Avoiding fraudulent email

13. Believing you won the lottery ... and other scam titles.

Spammers use a wide variety of clever titles to get you to open emails which they fill with all sorts of bad things. New email users often make the mistake of opening these emails. So in an effort to bring you up to speed, let me tell you quickly:

- You have not won the Irish Lotto, the Yahoo Lottery, or any other big cash prize.
- There is no actual Nigerian King or Prince trying to send you \$10 million.
- Your Bank Account Details do not need to be reconfirmed immediately.
- You do not have an unclaimed inheritance.
- You never actually sent that "Returned Mail".
- The News Headline email is not just someone informing you about the daily news.
- You have not won an iPod Nano.

14. Not recognizing phishing attacks in email *content*.

While never opening a phishing email is the best way to secure your computer, even the most experienced email user will occasionally accidentally open up a phishing email. At this point, the key to limiting your damage is recognizing the phishing email for what it is.

Phishing is a type of online fraud wherein the sender of the email tries to trick you into giving out personal passwords or banking information. The sender will typically steal the logo from a well-known bank or PayPal and try to format the email to look like it comes from the bank. Usually the phishing email asks for you to click on a link in order to confirm your banking information or password, but it may just ask you to reply to the email with your personal information.

Whatever form the phishing attempt takes, the goal is to fool you into entering your information into something which appears to be safe and secure, but in fact is just a dummy site set up by the scammer. If you provide the phisher with personal information, he will use that information to try to steal your identity and your money.

Signs of phishing include:

- A logo that looks distorted or stretched.
- Email that refers to you as "Dear Customer" or "Dear User" rather than including your actual name.
- Email that warns you that an account of yours will be shut down unless you reconfirm your billing information immediately.
- An email threatening legal action.

TOP 25 EMAIL SECURITY ISSUES



Future - Now

- Email which comes from an account similar, but different from, the one the company usually uses.
- An email that claims 'Security Compromises' or 'Security Threats' and requires immediate action.

If you suspect that an email is a phishing attempt, the best defense is to never open the email in the first place. But assuming you have already opened it, do not reply or click on the link in the email. If you want to verify the message, manually type in the URL of the company into your browser instead of clicking on the embedded link.

15. Sending personal and financial information via email.

Banks and online stores provide, almost without exception, a secured section on their website where you can input your personal and financial information. They do this precisely because email, no matter how well protected, is more easily hacked than well secured sites. Consequently, you should avoid writing to your bank via email and consider any online store that requests that you send them private information via email suspect.

This same rule of avoiding placing financial information in emails to online businesses also holds true for personal emails. If, for example, you need to give your credit card information to your college student child, it is far more secure to do so over the phone than via email.

16. Unsubscribing to newsletters you never subscribed to.

A common technique used by spammers is to send out thousands of fake newsletters from organizations with an "unsubscribe" link on the bottom of the newsletter. Email users who then enter their email into the supposed "unsubscribe" list are then sent loads of spam. So if you don't specifically remember subscribing to the newsletter, you are better off just blacklisting the email address, rather than following the link and possibly picking up a Trojan horse or unknowingly signing yourself up for yet more spam.

Avoiding malware

17. Trusting your friends email.

Most new internet users are very careful when it comes to emails from senders they don't recognize. But when a friend sends an email, all caution goes out the window as they just assume it is safe because they know that the sender wouldn't intend to hurt them. The truth is, an email from a friend's ID is just as likely to contain a virus or malware as a stranger's. The reason is that most malware is circulated by people who have no idea they are sending it, because hackers are using their computer as a zombie.

It is important to maintain and keep updated email scanning and Anti-virus software, and to use it to scan ALL incoming emails.

18. Deleting spam instead of blacklisting it.

An email blacklist is a user created list of email accounts that are labeled as spammers. When you 'blacklist' an email sender, you tell your email client to stop trusting emails from this particular sender and to start assuming that they are spam.

Unfortunately, new internet users are often timid to use the blacklist feature on their email client, and instead just delete spam emails. While not every piece of spam is from repeat senders, a surprising amount of it is. So by training yourself to hit the

TOP 25 EMAIL SECURITY ISSUES



blacklist button instead of the delete button when confronted with spam, you can, in the course of a few months, drastically limit the amount of spam that reaches your Inbox.

19. Disabling the email spam filter.

New email users typically do not start out with a lot of spam in their email account and thus do not value the help that an email spam filter can provide at the beginning of their email usage. Because no spam filter is perfect, initially the hassle of having to look through one's spam box looking for wrongly blocked emails leads many new email users to instead just disable their email spam filter altogether.

However, as an email account gets older it tends to pick up more spam, and without the spam filter an email account can quickly become unwieldy. So instead of disabling their filter early on, new internet users should take the time to whitelist emails from friends that get caught up in the spam filter. Then, when the levels of spam start to pick up, the email account will remain useful and fewer and fewer friends will get caught up in the filter.

20. Failing to scan all email attachments.

Nine out of every ten viruses that infect a computer reach it through an email attachment. Yet despite this ratio, many people still do not scan all incoming email attachments. Maybe it is our experience with snail mail, but often when we see an email with an attachment from someone we know, we just assume that the mail and its attachment are safe. Of course that assumption is wrong, as most email viruses are sent by 'Zombies' which have infected a computer and caused it to send out viruses without the owner even knowing.

What makes this oversight even more scandalous is the fact that a number of free email clients provide an email attachment scanner built-in. For example, if you use Gmail or Yahoo! for your email, every email and attachment you send or receive is automatically scanned. So if you do not want to invest in a third-party scanner and your email provider does not provide attachment scanning built-in, you should access your attachments through an email provider that offers free virus scanning by first forwarding your attachments to that account before opening them.

Keeping hackers at bay

21. Sharing your account information with others.

We've all done it – we need an urgent mail checked, and we call up our spouse or friend and request them to check our email on our behalf. Of course, we trust these people, but once the password is known to anybody other than you, your account is no longer as secure as it was.

The real problem is that your friend might not use the same security measures that you do. Your friend might be accessing his email through an unsecured wireless account, he may not keep his anti-virus software up to date, or he might be infected with a key logger virus that automatically steals your password once he enters it. So ensure that you are the only person that knows your personal access information, and if you write it down, make sure to do so in a way that outsiders won't be able to understand easily what they are looking at if they happen to find your records.

22. Using simple and easy-to-guess passwords.

Hackers use computer programs that scroll through common names to compile possible user names, and then send spam emails to those usernames. When you open that spam email, a little hidden piece of code in the email sends a message back to the hacker letting him know that the account is valid, at which point they turn to the task of trying to guess your password.

TOP 25 EMAIL SECURITY ISSUES



Hackers often create programs which cycle through common English words and number combinations in order to try to guess a password. As a consequence, passwords that consist of a single word, a name, or a date are frequently "guessed" by hackers. So when creating a password use uncommon number and letter combinations which do not form a word found in a dictionary. A strong password should have a minimum of eight characters, be as meaningless as possible, as well as use both upper and lowercase letters. Creating a tough password means that the hacker's computer program will have to scroll through tens of thousands of options before guessing your password, and in that time most hackers simply give up.

23. Failing to encrypt your important emails.

No matter how many steps you take to minimize the chance that your email is being monitored by hackers, you should always assume that someone else is watching whatever comes in and out of your computer. Given this assumption, it is important to encrypt your emails to make sure that if someone is monitoring your account, at least they can't understand what you're saying.

While there are some top-of-the-line email encryption services for those with a big budget, if you are new to email and just want a simple and cheap but effective solution, you can follow these step-by-step 20 minute instructions to install PGP, the most common email encryption standard. Encrypting all your email may be unrealistic, but some mail is too sensitive to send in the clear, and for those emails, PGP is an important email security step.

24. Not encrypting your wireless connection.

While encrypting your important emails makes it hard for hackers who have access to your email to understand what they say, it is even better to keep hackers from getting access to your emails in the first place.

One of the most vulnerable points in an email's trip from you to the email recipient is the point between your laptop and the wireless router that you use to connect to the internet. Consequently, it is important that you encrypt your wifi network with the WPA2 encryption standard. The upgrade process is relatively simple and straightforward, even for the newest internet user, and the fifteen minutes it takes are well worth the step up in email security.

25. Failing to use digital signatures.

The law now recognizes email as an important form of communication for major undertakings such as signing a contract or entering into a financial agreement. While the ability to enter into these contracts online has made all of our lives easier, it has also created the added concern of someone forging your emails and entering into agreements on your behalf without your consent.

One way to combat email forgery is to use a digital signature whenever you sign an important email. A digital signature will help prove who and from what computer an email comes from, and that the email has not been altered in transit. By establishing the habit of using an email signature whenever you sign important emails, you will not only make it harder for the other party to those agreements to try to modify the email when they want to get out of it, but it will also give you extra credibility when someone tries to claim that you have agreed to a contract via email that you never did.

For a quick primer on digital signatures, you can read YoudZone and Wikipedia's articles on the subject.

This article is intended to provide you with the basic information you need to avoid many of the email security pitfalls that frequently trip up new email users. While no single article can cover even the basics of email security, avoiding the 25 common mistakes listed in this article will make a dramatic difference in improving the safety and security of your computer, your personal information, and your emails.

TOP 25 EMAIL SECURITY ISSUES



Future - Now
