

7 Important Email Security Tips You Should Know About

Internet security is a topic that we all know to be important, but it often sits way back in the recesses of our minds, fooling ourselves into believing that "it won't happen to me". Whether it's the destructive force of the newest virus or just the hacking attempts of a newbie scriptkiddy, we're always only one click away from dealing with a security mess that we'd rather not confront. Nowhere is this truer than in our emails.



Mat Honan wrote a fascinating article over at Wired about Internet security and about how he became a victim of various online security flaws. In it, he wrote, "*[The] security lapses are my fault, and I deeply, deeply regret them*". He hits home on a very serious truth: in most of the cases where we face hiccups in security, we can trace the issue back to our own ignorance and negligence.

Safe online practices are important to keeping your online identity unadulterated and free from viruses, hackers, and all sorts of Internet-based shenanigans. And the best place to start? Your inbox.

Here are some simple yet important security tips you should know in order to keep your email account as secure as possible.

1. Use Separate Email Accounts

If you're like most people, your email account is probably the centralized hub of your personal activity. All of your Facebook notifications, website registrations, newsletters, messages, etc. get sent to your email box, right? That means you're putting all of your eggs in one basket - if that basket happens to fall, you'll lose all your eggs with it.

In other words, if you bring all of your activity into a single email account, what happens when someone breaks into it? I'd say it's plausible that they would gain access to everything else. This is why you should use multiple email accounts.

Having separate email accounts will not only help boost your security, but also your productivity. Imagine if you could consolidate all of your work emails into a single work account; all of your friends and family communicate with your personal account; you have a recreational account for various websites; and a throwaway account for potential spam links. This way, if someone hacks your work account, all of your personal emails are still safe.

2. Create a Unique Password



Going along with the multiple account idea, you should also have an entirely unique password for each of your email accounts. Even if you decide to keep one "master" email account, make sure that its password is 100% unique.

Using one password for all of your accounts is a rookie-level mistake. Suppose someone *did* hack into your personal email and they see all of your incoming Facebook notifications, eBay reminders, and more. Any half-wit hacker will test those accounts with the same password as your email account-and in your case, they would succeed.

This is common advice, I know, but so many people still neglect it. Admittedly, for the longest time, I too used the same password for literally every account that I had. When one of my friends figured out my password (without messing with anything, thankfully), I knew it was time to wise up.

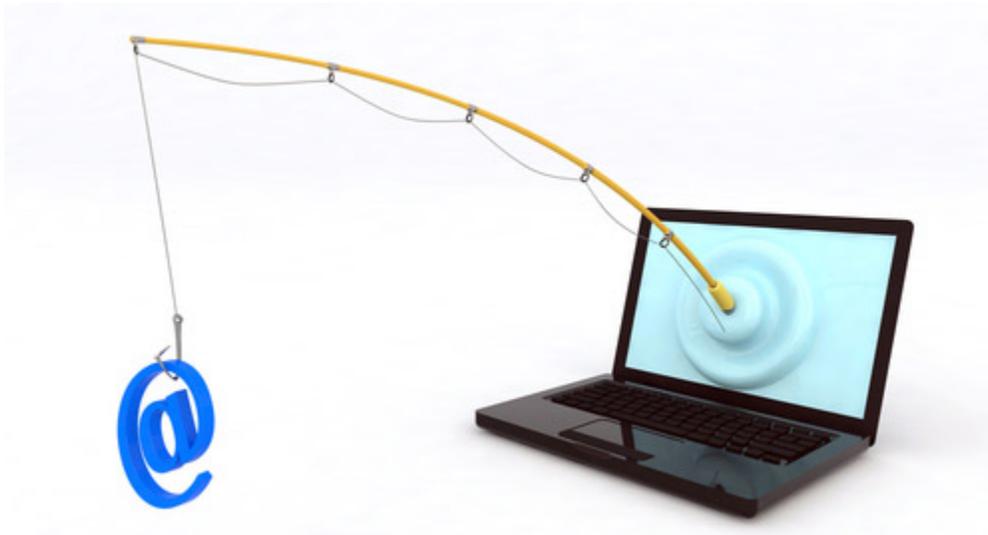
3. Beware Of Phishing Scams

When dealing with a particular company or product that requires account information, have you ever seen the following message: "Never give away your personal information? We will *never* ask you for your password." When someone sends you an email asking you for your personal information, you know right away that it's a trick.

But there's another level to this scam and it's called "phishing." Basically, malicious users will imitate and impersonate high-profile websites (e.g., eBay, Amazon, Facebook, etc.) and say that they're experiencing trouble with your account; all you have to do to fix it is to send them your username and password to verify your authenticity. Sometimes they'll even link you to a false website that looks *exactly* like the real thing.

Be wary. In fact, whenever your personal information is ever brought up in a non-face-to-face capacity, your scam detector should go off loud and clear.

4. Never Click Links in Emails



Phishing brings me to my next point. Whenever you see a link in an email, 99% of the time you should *not* click on it. The only exceptions are when you're expecting a particular email, such as a forum registration link or game account activation email. Things like that.

If you receive a spam email that tries to sell you a particular service or product, *never* click on *any* of the links inside. You never know where they'll lead you. Sometimes they might be safe; other times they'll bring you straight to the doors of hell and swarm you with malware and viruses.

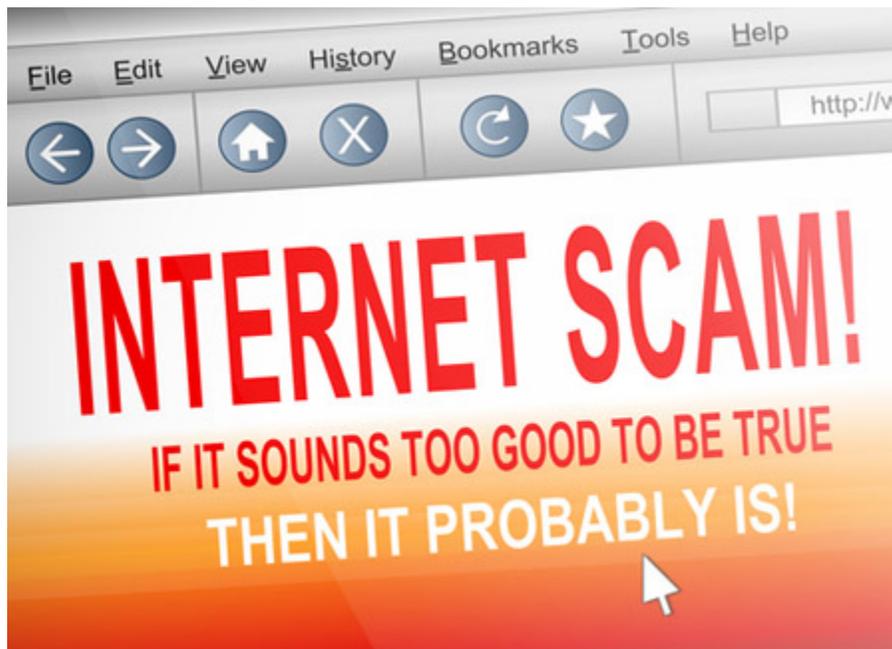
If you get an email from your bank or any other service (e.g., bill payments), always visit the website manually. No copy and paste. No direct clicking. You'll thank yourself later.

5. Do Not Open Unsolicited Attachments

Attachments are a tricky thing when it comes to email. If you're expecting something from a buddy or an uncle, then sure, go ahead and open the attachment. Have a laugh at the funny photo they sent you. It's all good when you *know* the person sending the attachment.

But if the email is unsolicited, *never* open any attachments. Even if the file looks innocent, you could be in for a world of hurt. Filenames can be spoofed. JPEGs could be EXEs in disguise and those EXEs will run as soon as they're downloaded. And then you'll have a virus on your hands.

6. Scan for Viruses & Malware



If you open an email and it seems suspicious in any way, go ahead and run a malware and virus scanner. Not every spam email will infect you with a virus and it may seem like overkill to run a malware scanner every time you open a fishy email, but it's better to be safe than sorry. The one time that you decide to let it go could be the time your computer loads a keylogger.

7. Avoid Public Wi-Fi

And lastly, avoid checking your email when you're on public Internet. Yes, I know that when you're waiting for an airplane to reach your gate, it can be tempting to whip out your smartphone or laptop and check for new messages. Unfortunately, public Wi-Fi can be extremely insecure.

There are programs out there called "network sniffers" that run passively in the background of some hacker's device. The sniffer monitors all of the wireless data flowing through a particular network - and that data can be analyzed for important information. Like your username and password.

It's strange that as the years go by, security grows tighter in some ways and we remain just as vulnerable as we've always been in other ways. Email security comes down to common sense and careful decisions. Don't let laziness and convenience overshadow your desire for protection and peace.