What to do if you receive suspicious emails

Basically if you get an email with no message or text explaining the link so just a link and nothing else - then be very sceptical, very sceptical. I always check the link using a tool called Short URL Scanner. Some links are pretty obvious others are often obfuscated. The email you receive may appear to be from a friend or name in the subject from someone you know or from an organisation you respect or know of. Sometimes the email name may have been slightly altered eg markbjames@outlook.com altered to markbjame@outlook.com. Do not assume it is to be trusted. The safest approach is to delete the email. If it is really important they will contact you again in a more formal way. As email and social media sites "merge" it is possible you may get an intrusion from a social media site so always be careful and scan your computer for malicious software regularly at a minimum weekly. (See attendix for recommendations on free tools to use).

Increasingly people's email contact lists are being hacked and stolen. Also once someone is hacked they have the whole of their contacts list for that account stolen and the perpetrator will send over a period on time several emails to different groups from the list of contacts so expect it to continue for some time.

If you receive an obviously suspicious email then do the following

1. Do not open the link or suspect file
2. Send an email to all the people on distribution of the email and the originator warning them of your suspicions.
3. Delete the email
4. Scan your system for malicious software.

How to Recover When You think you have been intruded

Norton Security recommends the following steps (full details of each item is in link below)

- ***Recognise the signs.***
- ***Notify friends.*** .
- ***Create a new email address.***
- ***Maintain an inventory.***
- ***Put online purchases on hold.***
- ***Make sure ALL your computer(s)and other devices (phones/tablets) are "clean".***
- ***Use your email user name wisely.***

Think this seems like a hassle? It's true that you'll have to do some recovery work, but the alternative can put you at risk for far bigger problems.

http://us.norton.com/yoursecurityresource/detail.jsp?aid=email_hacked ***(still active 14/08/2017)***

They omitted some other pieces of advice

1. If you are going to delete the "hacked" email account clear all the contents and contacts and then create a new email account preferably with GMAIL which has a good spam filter and picks up many of these spam emails.
2. Send an email informing all your contacts of your new email id and to ignore emails from your old email id explain you have had a problem and add the text above to every email contact in your hacked email id.
3. Use **strong passwords**. Use at least **ten** characters, including a minimum of one capital letter,one special character and two numbers in your passwords. A simple technique to help you chose a password try this technique. Use pairs of words

together but obfuscate them for example **Spain** and **strong** paired together but change the vowels to numbers. A=4 E=3 I=1 O=0 U=Q so " Spainstrong! " becomes Sp41nstr0ng! it contains a capital letter, more than two numbers with a special character ! and is twelve characters long

4. Use **different passwords** for **each** email account and **each** finance site, social network ids, forum accounts or shopping accounts. For information accounts such as weather, travel, holiday sites you can use a common but strong password for example **1Nf0rm4t10n%** if it is compromised you have lost nothing of value. Note do not use the example passwords listed above. Choose your own memorable words.
5. **Keep your passwords safe**, have a minimum of two copies but keep both well away from your computer and files. I keep my passwords in a password protected spreadsheet stored on two memory sticks that are password protected with a different password. **I also use a passwork system called Lastpass.**
6. **Be very sceptical** of links and files sent to you in emails without some clear indication of the sender and an appropriate explanation. If the link is obscured in some way i.e. turned into an "Subject" and hiding the actual URL (link) details. Bear in mind some spammers will make emails look as though they came from the person whose contact list was hijacked.
7. Finally, you can perform a scan on each of your computers on-line without needing to purchase a product. Here are some links:

http://housecall.trendmicro.com/uk/
http://www.bitdefender.co.uk/scanner/online/free.html
http://www.kaspersky.co.uk/downloads/virusscanner
http://home.mcafee.com/downloads/free-virus-scan
http://www.virscan.org/
http://www.f-secure.com/en/web/home_global/online-scanner

use a minimum of two sites to check out your computer(s).

If your email has been hijacked

This advice originated from http://www.switched.com/2011/02/24/what-to-do-email-account-hacked/ but I have made some modifications and additions.

Symptoms if you have been hacked:

- People listed in your e-mail contacts report being flooded with spam messages sent from your account. or
- you start receiving a bevy of "bounced" e-mails from random addresses you don't know. or
- You aren't able to log into your account or change its settings,
- you've discovered the settings have been altered. or
- You attempt to use e-mail, and find it has been blocked by your provider.

Diagnosis if you have been hacked:

Start with the obvious: If your password no longer works for your e-mail account (and it's definitely the correct password), you can be almost certain that someone else has taken control of it. And if your e-mail provider has blocked you completely, it's probably because your account was spewing out spam by the millions, forcing your provider to shut it down until you regain control. This is a good thing, and you'll get it back. Likewise,

learning from friends that your account has let loose a fire hose of spam (which sometimes can be verified by checking the Sent messages folder in your account) pretty much confirms that some scumbag has figured out your password. Losing control of your mail and password combo can be especially calamitous if, like far too many people, you use the same ones for all the online sites and services you use, such as social networking, banking and PayPal. Even the dumbest hacker will do a quick e-mail search in your account to scrape for login info on other sites, and, in no time, will assemble a pretty good portfolio on you. Depending on the ambition and skill set of the hacker, on the time between when your account was compromised and when you discovered it, and on how secure your various online accounts are, your level of pain may fall anywhere between minor annoyance to personal and financial meltdown. Time is of the essence, and don't underestimate how deep this thing can go.

Bounced messages are the digital equivalent of "return to sender, address unknown." On their own, bounced e-mails from strangers usually mean that a professional spammers has been sending spam with your e-mail address in the reply-to field (a process called "spoofing"), and hasn't actually breached your e-mail account. It's a crucial difference; having your account password compromised means your entire collection of e-mail correspondence has been exposed, while a spammers spoofing your address doesn't actually control anything. Unfortunately, while it's often possible to take back control of an infiltrated e-mail account (see below), once a spammers begins spoofing, you have no real recourse.

Causes:

While there aren't any hard and fast figures on what the number one cause of e-mail infiltration is, the overarching theme usually points to one extremely weak link: user behaviour. Despite the many ways an e-mail account can be hacked, the one common element is that you, the owner, essentially allows it by opening a Trojan link or attachment or protects it with a weak password or has their computer hacked via their IP address and a security flaw. More break-in options are listed below.

Every few years, studies show that the one reason spam is still so prevalent is because it actually works -- a percentage of naive users can always be expected to open a spam message, read it, and be tempted by whatever wares or schemes are offered. Of course, many of those e-mails (and sometimes pop-up windows from strangers on IM, Skype and similar apps) are actually phishing attacks that dupe recipients into believing they've been sent a legitimate message from a business or friend. Naive users will then reply with the requested login information.

A fair number of people also think nothing of checking their e-mail on a public computer -- in a library, electronics store or Internet cafe -- and simply neglect to log out. It's a momentary lapse of reason (particularly since I don't recommend checking e-mail on *any* public computer), and can be the equivalent of walking away from an ATM right after entering your password.

The other gargantuan user misstep is having weak, easily determined passwords, or using the same combination of login e-mail addresses and passwords across different sites. If a hacker breaks into one site, they can quickly try the same logins on *all* the popular sites -- to potentially devastating effect. But, before you beat yourself up, it's also possible that your login information has been stolen because your PC, or one you've used, has been infected with spyware or some other assorted malware.

Treatment:

Depending on the kind of hack you've been dealt, the treatment may be as simple as logging in, and changing your settings and password. Or it may entail agonizingly repeated attempts to lock out a persistent hacker, potentially killing off your account altogether. But you should never just give up and ditch the account without trying to deal with it first.

If you aren't able to log in, you're likely going to have to go through some frustrating hoop jumping. Conveniently, Twitter's help page has a handy list of links for all the major e-mail services' support pages.

Each service has its own method for determining that you are who you say you are, and are not the person who hacked -- or is planning to hack -- your account. Besides pre-set security questions, they may ask specific details about messages you've sent, and even the exact day you set up the account. If you don't have a copy of your initial registration e-mail, try contacting a close friend whom you would have e-mailed at the time, and ask them to dig into their archives for your early missives.

If you can log in:

1. Make sure your PC is current with all operating system (OS) updates and anti-virus/malware software. Also make sure all major software is up to date for example Skype, Web Browsers, Adobe, Firewall, Anti-virus, etc. Otherwise, if it has been infected by malware that spies on you, it will continue to transmit your info to whichever hacker has infiltrated your accounts. Use at least **two** on-line malware/virus scanners to check your PC and contents. (See list at the end If you aren't completely sure your PC is clean, then *don't* do any of the following. Any changes you attempt to make could be forwarded on by malware, too.
2. Depending on how your account has been abused, you may not need to contact everyone spammed by your hacked e-mail. (Your scam-savvy friends will recognize bogus messages as spam.) But, if there is a personal appeal for money -- saying you're stuck travelling and need cash, or are hurt and in a hospital -- or if malware was attached, you should send word to your contact list to delete those messages ASAP.
3. Set up at least two new e-mail addresses. Use your original e-mail address for personal or business communication as you'd normally do. The secondary e-mail address is insurance against future hacks; use it to communicate with your service provider, since many now ask for an alternative address as added protection. Then, use a third e-mail address only for registering for sites, newsletters, online shopping and other services. It may seem paranoid and excessive (hey, that's us!), but the idea is to compartmentalize your online life a bit. That way, each "world" has its own discrete e-mail account, and will minimize the damage that can be done by any future hacks. Most importantly, though: use a *different* and strong password for each account -- one that is at least six characters long, and is a combination of letters, numbers and capitals/lowercase.

It sounds difficult, but it isn't. It'll help prevent any hacker from gaining access to *all* of your data simply by infiltrating one site.

4. On a secure PC, log into your e-mail and then check whether or not any of the settings have been changed by a hacker. Smart hackers may set your account to notify them of any changes, so that they can go back in and switch things again. Check whether or not a signature has been added, and whether your account has been set to forward e-mail to another address that isn't yours or to run a filter that automatically forwards e-mails or attaches a file. If any of those settings have been altered, delete the new settings.
5. Once you have changed the settings, create a new password, and add your secondary e-mail account as your alternative address.
6. Going forward, never list your main e-mail address publicly anywhere online -- in forums, in online ads, on blogs or any place where they can be harvested by spammers. Use only your "registration" address, and keep it separate from your main address book. You can list it in an obscure way see my example at the bottom.
7. Don't use public computers to check e-mail; there's virtually no way to know if they are infected with malware accidentally, or have keylogging spyware installed intentionally. But if you absolutely must use e-mail on a public computer, set up an extra account before you leave and change the password regularly.

Best of luck
Mark Drew
email: mark1drew at googemail dot com
Last updated: 14th August 2017 at 15:02 CET

APPENDIX - Free tools

Online tools

http://housecall.trendmicro.com/uk/
http://www.bitdefender.co.uk/scanner/online/free.html
http://www.kaspersky.co.uk/downloads/virusscanner
http://home.mcafee.com/downloads/free-virus-scan
http://www.virscan.org/
http://www.f-secure.com/en/web/home_global/online-scanner

Download tools

www.avg.com/**free-antivirus-download**
www.avira.com/en/avira-**free-antivirus**
avast.en.softonic.com
uk.norton.com › Free Trials
home.mcafee.com/store/**free-antivirus**-trials
usa.kaspersky.com/**download**s/**free**-home-trials/**anti-viru**

Remember there are other tools available such as scanners for malware, tools for tablets and phones.

END OF DOCUMENT