UNDERSTANING VIRUS AND MALWARE INFECTIONS IN EMAILS?

A short information pack for the office worker or user working with emails every day (Non-Technical, so we can all understand)

WHAT IS SPAM?

HOW DO YOU KNOW IF YOU HAVE BEEN INFECTED?

HOW IS MY PC INFECTED BY SPAM?

HOW MY PC INFECTS OTHERS

HOW CAN I FIX MY PC, AND OTHERS INFECTED?

POPULAR ANTI-VIRUS AND ANTI-MALWARE SOFTWARE

WHAT HAPPENS AFTER PC HAS BEEN CLEANED?

ABOUT BLACKLIST CHECK

Do not trust FREE anti-virus software.
Purchase the full paid version.
At the end it is worth it.

INSTALL QUALITY ANTI-VIRUS AND ANTI-MALWARE SOFTWARE ON ALL YOUR PC's, LAPTOPS, TABLETS AND SMARTPHONES.

DO NOT CLICK ON LINKS IN EMAILS WHICH ARE NOT ADDRESSED TO YOU OR YOUR COMPANY, OR SUSPICIOUS ATTACHMENTS TO UPDATE YOUR PASSWORD OR EMAIL. YOUR I.T. SUPPORT OR WEBMASTER WILL SEND YOU ANY EMAIL ISSUES.

WHAT IS SPAM?

Irrelevant or unsolicited (unrequested, unwelcome) messages sent over the Internet, typically to a large number of users, for the purposes of advertising, phishing, spreading malware, etc. by SPAMMERS (Cyber Criminals)
Phishing email messages, websites, and phone calls are designed to steal money. Cybercriminals can do this by ***installing malicious software on your computer*** or stealing personal information off of your computer.

Malware is a contraction / infection of ***malicious software***. Put simply, malware is any piece of software that was written with the intent of doing harm to data, devices or to people. When you hear talk of viruses, Trojans, spyware and the like, what you're really hearing is talk of ***different kinds of malware***.

HOW DO YOU KNOW IF YOU HAVE BEEN INFECTED?

Emails you send out are bounced back by remote email server, informing you that you are blacklisted. Other users does not receive your emails, and remote users complain that they cannot send emails to you, as you have been blacklisted. You receive a bounce email with error 550 Message rejected - You are blacklisted.

Your PC is Infected

Send SPAM

Mail server detects SPAM Blacklist you

Remote Mail server detects SPAM, sends ERROR message back, You have been Blacklisted

HOW IS MY PC INFECTED BY SPAM?

You have not taken the proper precautions by ***installing proper anti-virus and anti-malware software on your Desktop, Laptop, Tablet or Smart Cellphone***. This makes it easy for the SPAMMERS to install malicious software on your device, and take control of it. This malicious software is sent to you with an "innocent looking" email. If your defence is not good, this sofware will slip through and install on your PC.

Beware of links in emails. If you see a link in a suspicious email message, don't click on it. Rest your mouse (but don't click) on the link to see if the address matches the link that was typed in the message. In the example below 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***.

Link example:
https://www.woodgrovebank.com/loginscript/user2.jsp

malicious website

Hover over link = http://192.168.255.205/wood/index.htm

Do not click on any such link, as this is all that is required by the SPAMMER to download malicious software onto your device. ***DELETE this email.***

Beware of attachments in emails

Do not just click on any attachment in a received email. If you don't know the company or transaction, rather DELETE it. If you click on such a JPG, PDF, WORD, EXCEL, Swift pdf.iso or .EXE extension attachment, it could be embedded code infecting your device. Also beware of a .txt file extension. Could be malicious.

DO NOT CLICK ON ANY ATTACHMENT OR LINK, UNLESS YOU ARE SURE ABOUT THE SENDER

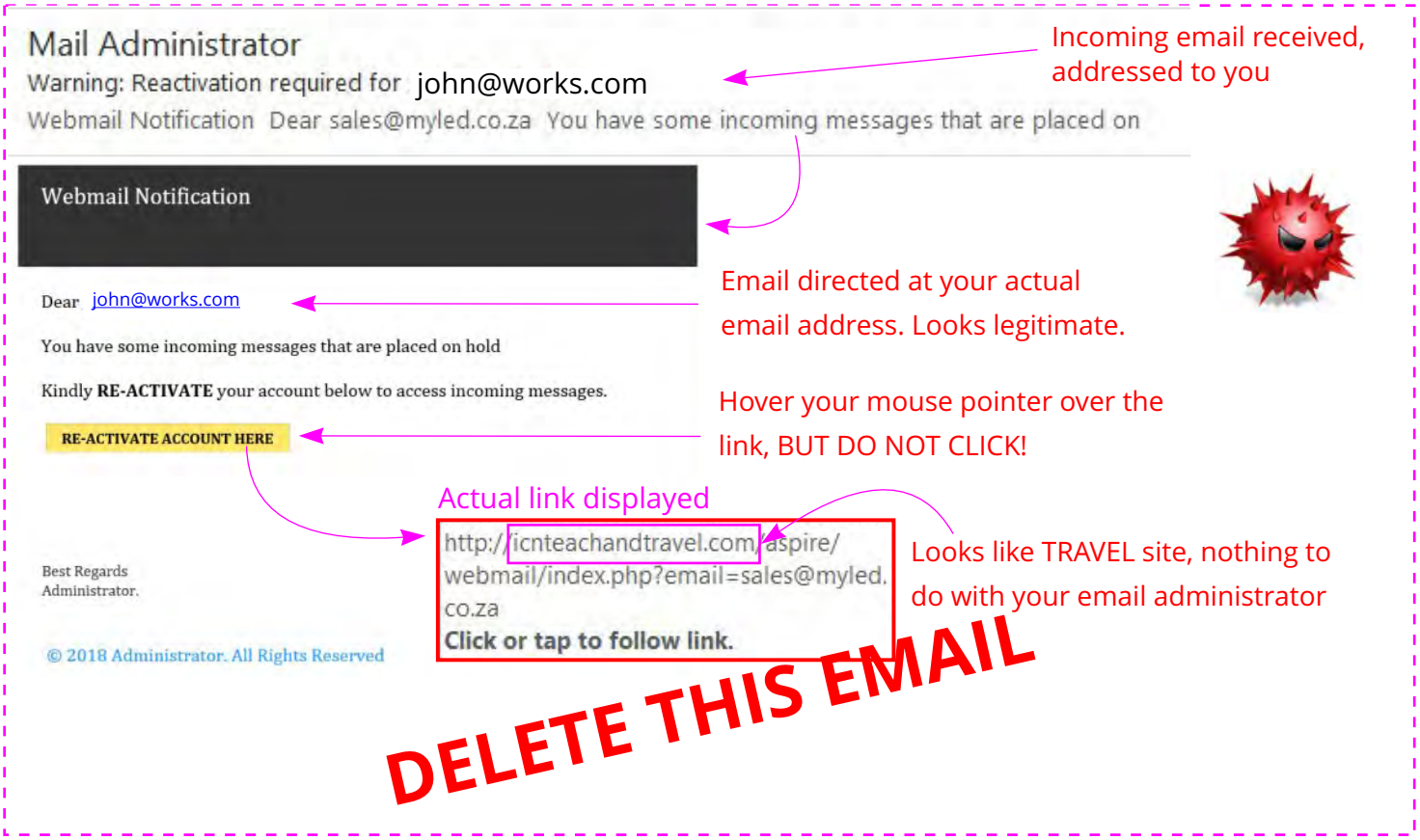
ALWAYS keep in mind that ***the SPAMMER wants you to click on the link or attachement.*** Some emails looks very authentic, just like a real request from the Bank or Company you are familiar with. ***ALWAYS be suspicious!!***

EXAMPLES OF PHISHING EMAILS

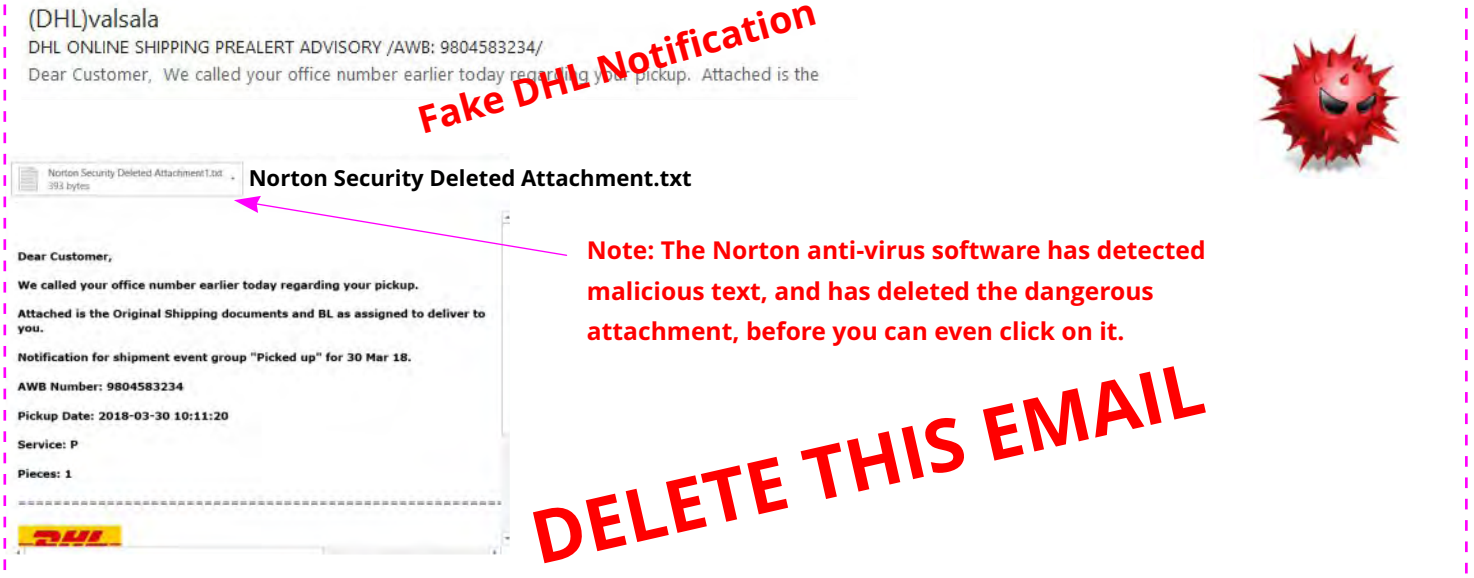
Email requesting a click to collect your private data or to download malicious software onto your PC.

You receive this innocent looking email to **reactivate your email account**.
YOU WILL NEVER BE REQUEASTED THIS BY YOUR REAL ADMINISTRATOR, AS THERE IS NO SUCH COMMAND. BE CAREFULL AND DELETE THIS EMAIL.

Phishing mail example 1



Phishing mail example 2

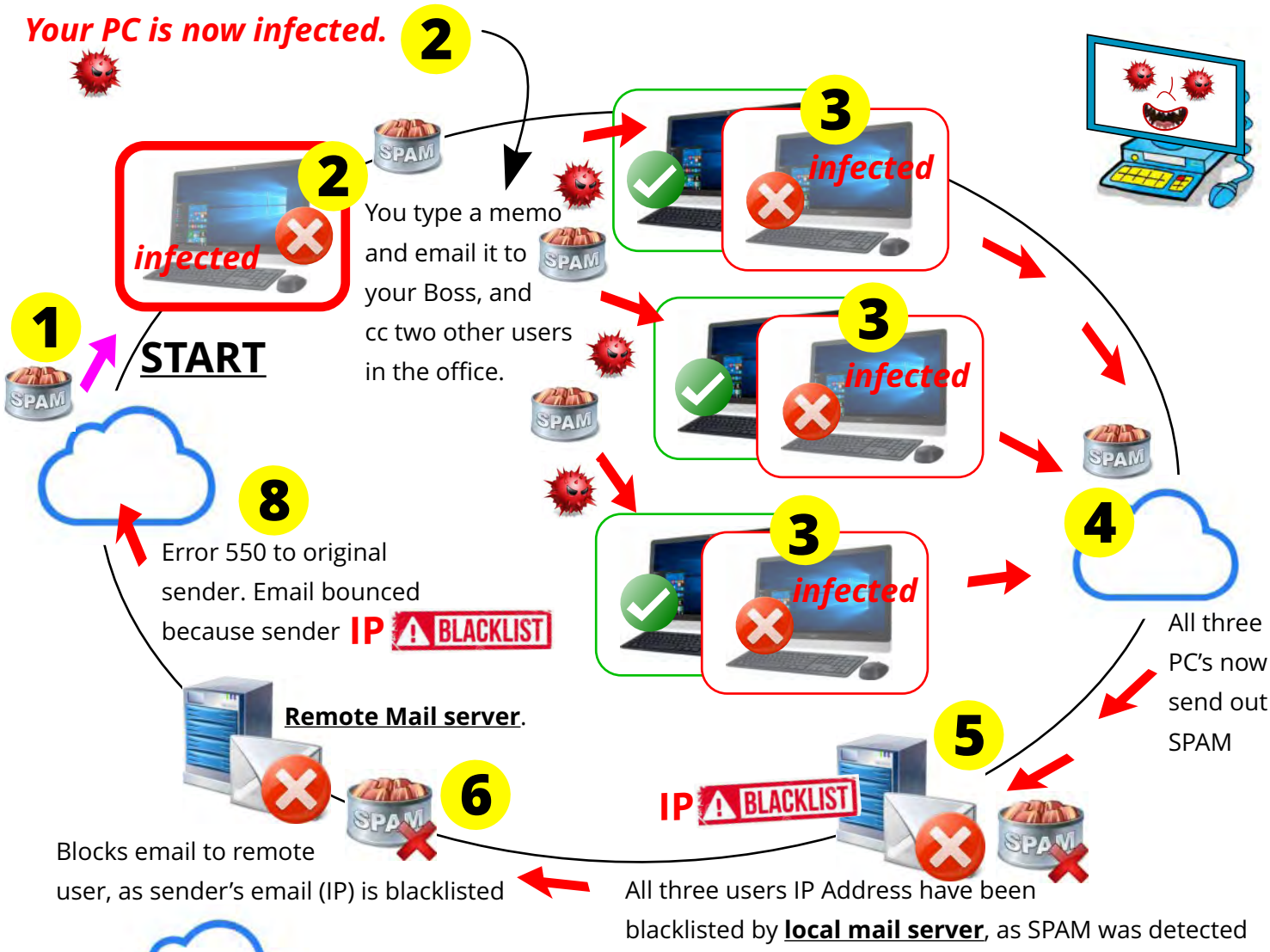


HOW MY PC INFECTS OTHERS

(If no proper protection is installed)

1 You ***receive malicious software in an email attachment***. Your PC. You click on the attachment, and the malware is downloaded and installed on your PC.

Your PC is now infected.



SPAM is messages sent over the Internet, typically to a large number of users, for the purposes of advertising, phishing, spreading malware, etc. by SPAMMERS (Cyber Criminals)

Follow the numbers: 1 - 7

1. SPAM directed at your email address.
2. You click on innocent looking email attachment, and malicious software is downloaded and installed on your PC, laptop, tablet or smartphone.
3. You email a memo to your Boss and two colleagues, and your infected email is downloaded on all 3 PC's.
   The three PC's are now infected.
4. Three PC's now send out SPAM from their email accounts.
5. Mail server detects this SPAM, and blacklist the email addresses (IP's).
6. If mail is passed through, the remote mail server could have blacklisted email /IP addresses. Error message is passed back to the original sender - You are blacklisted.
7. Remote recipient does not received email.

HOW CAN I FIX MY PC, AND OTHERS INFECTED?

(If no proper protection is installed)

When you realise that someting is wrong with your email, and or you receive a notification [ERROR Message] that your email (IP address) has been blacklisted, please do the following:

1. No use complaining to your email service provider / administrator, that you have been blacklisted. There is nothing they can do, other than advise you on the following.
2. Request your IT support technician to do an in-depth scan on your desktop PC, laptop, tablet or smartphone. Keep in mind that any device which you have setup to send and receive emails, and view websites could receive and install malicious software.
3. Always ensure ***top quality anti-virus and anti-marware software is installed*** on your device. Do not just go for the FREE version, as the performance is not as good as paid anti-virus and anti-malware software.
4. This software must be permanently installed on all devices, and updated regularly as new updates becomes available. It only takes one missing update, and a new dangerous virus can infect your PC. Remember, the SPAMMERS NEVER give up. This is their business, and livelihood.
5. Below are popular antivirus and malware software available in the industry. Each IT Tech has his/her own choice of "the best". Make your choice.

Popular antivirus and malware software

Product	McAfee AntiVirus Plus	Symantec Norton AntiVirus Basic	Webroot SecureAnywhere AntiVirus	Bitdefender Antivirus Plus	Kaspersky Anti-Virus	Advanced SystemCare Ultimate 11	Malwarebytes
Lowest Price	$19.99 McAfee	$19.99 Symantec	$18.99 Webroot	$19.99 Bitdefender	$29.99 Kaspersky Lab	$19.99	$39.99
Editors' Rating	EDITORS' CHOICE	EDITORS' CHOICE	EDITORS' CHOICE	EDITORS' CHOICE	EDITORS' CHOICE		

WHAT HAPPENS AFTER PC HAS BEEN CLEANED?

The email servers and blacklisting directories monitors all blacklisted IP addresses, and will remove the blacklisting as soon as the SPAM source is no longer there, in most cases of low level infections.

Popular site to check blacklisting: https://mxtoolbox.com/blacklists.aspx

ABOUT BLACKLIST CHECK

The blacklist check will test a mail server IP address against over 100 DNS based email blacklists. (Commonly called Realtime blacklist, DNSBL or RBL). If your mail server has been blacklisted, some email you send may not be delivered. Email blacklists are a common way of reducing spam. If you don't know your mail server's address, start with a MX Lookup.

When the email (IP address) address has been cleaned of SPAM, in some cases the mail servers will remove the low level blacklisting TAG automatically within 24 - 48 hours, or longer, depending on the server, as there might be more than one.

If this does not work, you might have to get your IT Tech to help you identify the servers where you have been blacklisted, and work with your IT Tech to remove the blacklistings one by one from your IP address.

CONCLUSION

Many users or companies ignores virus and malware infections, or only installs the FREE anti-virus versions, only to be crippled when the whole office PC network has been infected. At this point it could seriously affect the production of a user or a company.

Keep focus on "***protection***" for all your devices, and it would remove this stress issue from your workplace.

Install proper anti-virus and anti-malware software on your Desktop, Laptop, Tablet or Smart Cellphone, and RENEW your subscriptions every year.