

# Tame Your Email How To Control Spam and Master Your Email

---

**Copyright © 2004 Dan Butler**

This excerpt is from the full book Tame Your Email. If you like the information you can find more information on the complete book visit:

<http://www.TameYourEmail.com>

Find more helpful productive information like this in the TNPC Newsletter:

<http://www.tnpcnewsletter.com/>

**Disclaimer:** The author of this manual has tried to present the most accurate information to his knowledge at the time of writing. The author of this book shall not be held responsible for any kind of losses or damages caused by its use and implementation. If any legal or technical advice is needed, consult with appropriate professionals. All software recommended in this book has been used and tested by the author on his personal computer systems. The book's author shall not be held responsible for any damages or loss of data caused by using the recommended software on your system.

No part of this book may be reprinted, electronically transmitted or reproduced in any way without prior permission from the author under the penalties of Federal Copyright Law.

To report unlawful distribution of this book please contact:

[Dan@TameYourEmail.com](mailto:Dan@TameYourEmail.com)

**Tame Your Email**

**ISBN 0-9708631-3-6**

**Dan Butler  
Box 79230  
Saginaw, TX 76179**

**© 2004 Dan Butler**

**All Rights Reserved**

<b>HOW TO USE THIS BOOK .....</b>	<b>9</b>
Contents Pages .....	9
Navigation .....	9
Navigational Panel .....	10
Turning Pages .....	11
Returning to Previous Pages.....	11
Watching the Movies .....	11
<b>EMAIL CLIENTS REVIEWED.....</b>	<b>12</b>
Microsoft Outlook Express .....	13
Microsoft Outlook .....	14
Mozilla Thunderbird.....	15
Eudora.....	16
Pegasus Mail.....	17
The Bat!.....	18
Popcorn.....	19
Summary .....	20
<b>TOP TRICKS FOR TAMING EMAIL YOU SEND .....</b>	<b>20</b>
<b>One Topic per Email.....</b>	<b>20</b>
<b>Maximize Your Subject Line.....</b>	<b>21</b>
State the topic of your email.....	21
How DNO will cut your time in half .....	22
Why ... Will Get Your Message Read .....	24
<b>Quote Efficiently .....</b>	<b>25</b>
Above or Below .....	25
<b>Put your main message in the first paragraph .....</b>	<b>27</b>
<b>Second paragraph: Says what you want done when they read the email.....</b>	<b>28</b>
<b>Rest of the email: Details.....</b>	<b>29</b>
<b>Subject Line Prefixes .....</b>	<b>31</b>

<b>The Two Minute Rule.....</b>	<b>32</b>
<b>Summary of Sending Mail Tips .....</b>	<b>32</b>
<b>TOP TRICKS FOR TAMING YOUR INCOMING EMAIL .....</b>	<b>33</b>
<b>Use Rules to Simplify Your Life .....</b>	<b>33</b>
Creating a Rule .....	33
Highlight important messages .....	38
Color Code your Inbox .....	39
Delete Certain People .....	39
Mailing Lists.....	39
Filing Your Mailing Lists .....	42
<b>Edit Your Subject Lines .....</b>	<b>43</b>
<b>Should you forward that email?.....</b>	<b>43</b>
<b>Summary of Incoming Email Tips.....</b>	<b>44</b>
<b>PROGRAMS FOR SIMPLIFYING YOUR LIFE.....</b>	<b>45</b>
<b>Keyboard/Macro Tools.....</b>	<b>45</b>
<b>Search Tool.....</b>	<b>49</b>
X1.com .....	51
<b>TAMING SPAM AND OTHER UNWANTED EMAIL .....</b>	<b>51</b>
<b>What is Spam .....</b>	<b>52</b>
Attempts at Identity Theft .....	53
Virus Propagation.....	55
Forwarded Jokes(?) .....	55
<b>Short Course on Spam.....</b>	<b>56</b>
Spam vs. Newsgroups .....	56
How Spammers Get Your Address .....	57
Why Spam in Your Inbox is Not Addressed To You.....	58
How Spammers Hide Their True Address.....	59
How Your Email Reader May Reveal Your Address .....	61
Some Definitions of Spam.....	62
Spam Horror Stories!.....	64

<b>Choosing your email address .....</b>	<b>66</b>
Avoid common names by themselves .....	67
Put Two Common Words Together .....	67
Avoid hard to spell words .....	67
Make it easy to remember .....	67
Spam proofing your address .....	68
Can you still use munging to get past the Spambots? .....	69
<b>Spam fighting.....</b>	<b>69</b>
Your ISP's filters.....	69
Intermediate filters at your ISP .....	70
A Spam Fighting ISP I Recommend:.....	70
Intermediate filters on your Local PC .....	71
Your mail clients filters .....	71
Your Eyes.....	71
Summary .....	71
Measuring Your Effectiveness.....	72
False Positives and False Negatives .....	72
<b>Types of Filters .....</b>	<b>73</b>
Whitelisting and Blacklisting .....	73
Challenge/Response .....	73
Prescreening .....	74
Bouncing Spam .....	75
Blacklists .....	76
SpamCop .....	76
Bayesian Filters.....	77
<b>PRIVACY AND SECURITY.....</b>	<b>83</b>
Which Programs Leave You Most at Risk? .....	84
What Your Browser Tells About You .....	84
Advertisers and What you Tell Them .....	87
Protecting Your Sensitive Data .....	90
PGP Questions & Answers .....	91
PGP vs. Certificates .....	94
Hide Sensitive Data in Plain Sight.....	94
Assorted Ideas on Security .....	97
Sending Encrypted Email .....	99
PGP - Protecting Your Files .....	101
PGP - Protecting Many Files at Once.....	103

<b>Conclusion.....</b>	<b>104</b>
<b>Glossary .....</b>	<b>104</b>
<b>About Dan Butler .....</b>	<b>107</b>

## Attempts at Identity Theft

Some of your spam will be blatant attempts at identity theft. Ever receive an email claiming to be from PayPal wanting you to verify some information? It's most likely a forged email trying to get a hold of your password.

Here's how it works. You click the link in the email. A website pops up that looks like PayPal. You log in. The thief now has your PayPal username and password. How long do you think it will be before your account is at \$0? And the other information you have up there may be being used against you as well. It's a nasty scam that takes in many people. I almost fell for it myself.

I have seen the same scam being run claiming to be eBay, PayPal, Western Union, and several online banks.



**Note: The video was not included in this document to save on space. The full book contains many videos to show exactly how to use the tips in this book.**

So how do you protect yourself? In this case it's easy. If you receive an email wanting you to verify any information – don't click the link in the email. Instead go directly to the companies website with your web browser. You will know you are at the right place and you can check your information from there.

If you do click the link in your email be sure to look at the location line in your browser to see where you really ended up. Chances are it's a fake address appearing to be the actual site. Everything will look right.

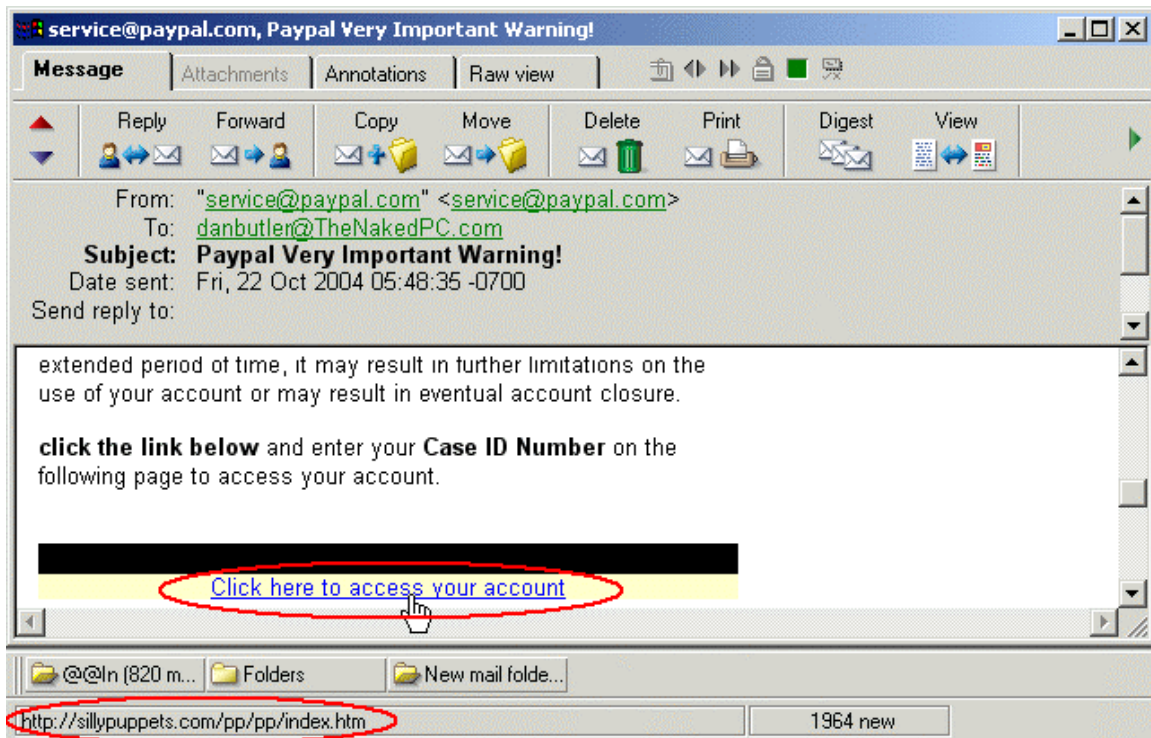


Figure35: Sample Phishing Email

Look at this picture. It's an email pretending to be from PayPal. The link says "Click here to access your account". If you look at the Status bar you see the URL points to "http://sillypuppets.com. If you followed the link you would put your account and its money in jeopardy.

I want to be clear on this. Do not click links in your email asking you to confirm your account information. Instead open your web browser and type in the address of the service. If you are still unsure after you log in from the official web site contact the company by telephone. You can't be too careful with your sensitive information.

If you receive Phishing emails claiming you have won a lottery simply run a Google search on the name of the company sending you the email. You will learn very quickly if you have a legitimate offer or not.

You can report the Phishing email to the spoofed company. Simply go the web site and look for an address to forward abuse mails to. Normally this address is abuse@companyname.com . Your email will probably not be read by a live human. If a Phishing run has been sent the company may receive thousands of complaints in a very short time.

## Virus Propagation

Viruses are frequently passed from machine to machine using email. Often the virus will claim to be an important update. Other times it will claim to be a list of some sort. Occasionally you will get an email asking if you can read the document. Or supplying you with a password to read the attachment. If you don't know the person sending the document or you aren't expecting an attachment from anyone don't open it. Instead run it through your virus scanner. Most modern virus scanners are able to scan your email as you download it. I do recommend you run your scanner on incoming email. I am indifferent on scanning outgoing email.

The anti-virus programs I like best are AVG and F-Prot. AVG has a free version and F-Prot is reasonably priced for yearly updates. If you like AVG I would recommend going ahead and paying for the full version. You can find more about these programs here:

<http://www.f-prot.com/> <- Information on F-Prot Anti-Virus

<http://grisoft.com/> <- Information on AVG Anti-Virus

## Forwarded Jokes(?)

One area that borders on spam is forwarded jokes. You know the ones that make the rounds. All of us probably have one or two people who forward all the latest jokes around. I don't usually read them and find them to be a slight nuisance.

If you are one who likes to forward the jokes around take a few moments to strip all the extra forwarding information and old emails from the message before you send it. It keeps you aware of how other people's addresses are treated.

If you have someone who routinely forwards these items with all the addresses free and clear, drop them a note and let them know the better way to work. We talked about forwarded jokes and warnings in the *Should You Forward That Email* section of the book.

Here is what I send to people who forward hoaxes and Urban Legends:

Dear Friend,

Thank you for thinking of me when you find these warnings. Unfortunately the warning you forwarded is a hoax. You can read more about it here:

<http://www.example.com/hoax-info> <- use the actual URL for information!

Please make sure the warnings are valid before you forward them to me.

Thank you.

**Here is what I send to people who insist on forwarding all the latest jokes:**

Dear Friend,

Thank you for taking the time to keep in touch with me. Unfortunately I receive so much email it is difficult to keep up. Can you please remove me from the list of people you forward jokes to?

I appreciate it.

## ***Glossary***

**Access Provider** – a company that connects your home computer to the Internet.

**ADSL** – Asymmetric Digital Subscriber Line high speed phone line service.

**Autoresponders (Mailbots)** – Automated programs which are established to return a prewritten message upon receipt of e-mail.

**Backup** – a copy of your files for use in case of an emergency. Can be a copy of your whole system or just the important files.

**Bayesian** – a statistical formula. Used to analyze incoming email and determine if it is spam.

**Blacklist** – List of addresses that you will not accept email for.

**Bounce** – A returned, can't deliver e-mail message.

**Browser** – an application used to view the World Wide Web.

**Challenge/Response** – A system that asks you to prove you are a real sender before it will deliver your email.

**Context menu** – menus accessible by right-clicking inside of an application. Changes according to the current context.

**Dialog box** – a box containing information or options for you to fill out. Most often used to customize applications and report system status messages.

**Directory** – see folder.

**Double-click** – quickly clicking the left mouse button twice on the same object. Can be adjusted in the Control Panel / Mouse applet.

**Download** – transferring a file from a remote computer to your computer. Usually done with FTP. Sometimes called GET.

**Explorer** – an application for exploring the file system in Windows.

**Folder** – a named space on a computer disk for storing files.

**FTP – File Transfer Protocol** – Used to transfer files from one computer to another over the Internet.

**Full Backup** – a complete copy of all the files on your system for use in case of an emergency computer failure.

**Header** – The first part of an email message which contains information about the routing of the message during delivery over the Internet.

**HTML** – Hypertext Markup Language. Used to format Web pages for the Internet.

**IMAP** – Internet Mail Access Protocol. An emerging standard for Internet email.

**ISP** – Internet Service Provider. A company which links your computer to the Internet.

**Left-click** – using your left mouse button to select an object.

**Left-drag** – dragging an object using your left mouse button.

**Mailing List** – A collection of e-mail addresses of people who have asked to receive regular mail discussions on a particular topic.

**Mailing List Manager** – An automated program to handle the administrative functions of a mailing list.

**Moderator** – Someone who controls the postings of messages in a Mailing List to ensure conformity with the topic and list policies.

**Newsgroup** – name given to Usenet groups.

**NNTP** – Network News Transport Protocol. Used to transmit Usenet news around the Internet.

**Phishing** – Emails disguised to look like official requests for information from financial institutions. Really an attempt to collect personal information for identity theft.

**POP** – Post Office Protocol. A standard for receiving Internet email. See also IMAP and SMTP

**Protocol** – A set of rules and conditions which perform a certain function. Usually used to have computers talk to each other. See also FTP, POP, IMAP, NNTP, SMTP, and TCP/IP.

**Right-click** – using your right mouse button to select an object by clicking and releasing the right button..

**Right-drag** – dragging an object using your right mouse button.

**Signature** – 4 - 8 lines of text placed at the end of a mail message with the author's contact information, favorite quote, special of the month, autoresponder/web site address, etc.

**SMTP** – Simple Mail Transport Protocol. Used for sending Internet mail.

**SPAM** – unsolicited bulk e-mail. Sent to people who didn't ask for the email and typically with forged contact information.

**Subject Line Message** – an email message contained entirely on the subject line.

**Subscription** – means you are a member of an Internet mailing list. Often free.

**System Tray** – the small area on the right end of the Task Bar where system level programs display their icons.

**Task Bar** – runs across the bottom of the Windows 98 screen. Contains the Start Menu, Toolbars, Running Programs, the System Tray, and optional Toolbars. See Chapter 06 'Going Further with Additional Customizations'.

**TCP/IP** – Transmission Control Protocol/Internet Protocol. A standard set of networking protocols that tie the Internet together.

**UBE** – Unsolicited Bulk Email.

**UCE** – Unsolicited Commercial Email.

**URL** – Uniform Resource Locator. An addressing schema for Internet sites.

**Usenet** – a series of many thousands of message boards on the Internet.

**Virus** – a malicious program that destroys data.

**Whitelist** – a list of addresses you will accept email from.

**WWW** – World Wide Web, the graphical part of the Internet.

### ***About Dan Butler***

Dan Butler has been involved with the Internet and email since 1992. He is the author of *Strange Happenings*, *Slightly Strange*, and co-author of *The Book That Should Have Come With Your Computer*, and *The Unofficial Guide to PC's*. His award winning articles have

appeared in magazines and newsletters. He is currently Editor-in-Chief of the award winning TNPC Newsletter.

Dan currently makes his home in Saginaw, TX where he lives with the love of his life Kelley, and their ten children.

Did you find the information in the book helpful? Why not get a copy of the whole book. Just go to:

<http://www.tameyouremail.com/>