

Business/News & Views®

Technology Tips

By [StaffTechAlert](#)

Keeping Receipts

Keeping physical paper receipts can be a hassle. Where do you store them? How long do you keep them? What if they fade? Technology offers an easy solution: Digital cameras. Just take a quick snapshot of a receipt and store it on your computer. Now you don't have to worry about it getting lost or damaged. Or use your mobile phone's camera and email it to yourself. What if your computer crashes? Storing the receipt images in an online backup like [Online File Folder](#) ensures their safety.

How to Tell a Forged Email from a Real One

If you're like most people, about 90% of the mail that comes to your personal inbox these days is unwanted — from seemingly harmless sales emails to viruses disguised as the latest joke or gossip. Fortunately, there are a few good techniques to use when determining if an email is legitimate.

One of the most obvious methods is looking at the "From:" address. It is not going to be the spammer's real email address; that would be too easy to trace back to them. Instead, they will use a fake address or a real address that is not connected to them. And to give their email the best chance of getting through, spammers will choose a common domain, such as @hotmail.com or @yahoo.com. No anti-spam service can block a domain that produces so much legitimate email.

Another place to look is the grammar, spelling and even the words used. Emails coming from large, legitimate companies are proofread before they are sent; a badly written email should be a red flag. Along those same lines, large companies generally do not use multiple exclamation points (!!!!!) or casual words (Hey, Yo, Dude) in their communications. If a word or phrase seems out of place, be suspicious.

Finally, be aware of what the email wants you to do. If it has an attachment, assume it is a virus. It is safer to make that assumption than it is to take your chances by clicking it. If there is a link in the email, roll your mouse pointer over it without clicking. Most email programs will show you where the link will take you. If you get an email that claims to be from a legitimate company, but the link goes to a site you've never heard of, you should investigate further before clicking.

These types of emails would not be so common if they weren't working. If we all spent a little more time looking before we leaped, we would not only stay safer, we would also reduce the amount of spam that's sent.



Let me know if you have any comments, questions, or suggestions.

Write David W. Weatherholt at david@bnewsviews.com

A. 10600 Cutter Circle Anchorage, Alaska 99511-0385 USA T. 907.360.9241 F. 888.731.1093

E. david@bnewsviews.com W. www.waconsult.com