COMPUTER NEWS from the

SEPTEMBER 2013 Volume 1 NO. 6

As found on the web and other sources.

Are You a Victim of CatPhishing?

From: “askbobtankin.com”.

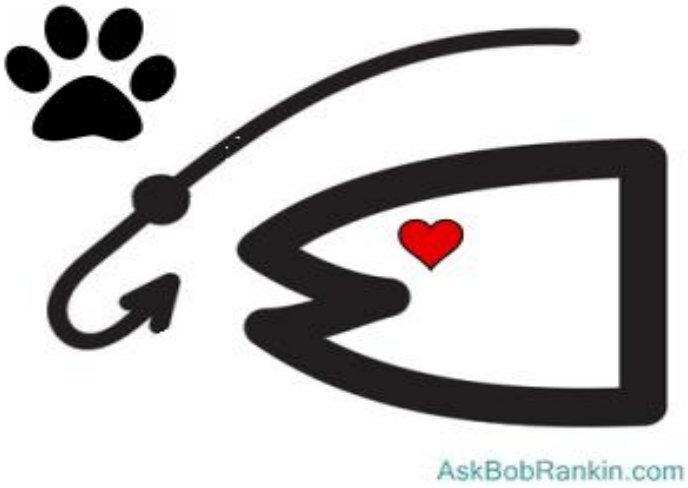
'I have known men to fall in love by light so dim they would not choose a suit by it,' wrote Ambrose Bierce many years ago. Today, the light is not only dim but deceptive. Lonely people of all persuasions are at increasing risk of being preyed upon by phony romantic partners who not only aren’t what they seem to be, but may not exist at all! Read on to learn about catphishing...

What is CatPhishing?

San Diego Chargers linebacker Manti T’eo was the victim of such a cruel hoax. The All-American football player fell in love with a “woman” sight unseen through social media. The sports press made much of Manti’s dedication to “Lennay Kekau,” purportedly a Stanford University student who tragically died of leukemia.

But “Lennay” turned out to be a hoax, a fictitious personal elaborately crafted by a male acquaintance of Manti’s. This cruel trick was just a joke that went too far; but there are cases in which the love-smitten have been scam-bitten.

The practice of using a fake virtual persona to dupe a victim out of money (or just inflict emotional damage) is called “catphishing.” The neologism seems to be a play on “phishing” (using deceptive email to obtain sensitive information) and a Southern sport called “noodling,” in which large catfish are patiently enticed into chomping down on a probing hand which hauls them into the boat. Jeff Foxworthy meets the Internet!



Catphish lurk on dating sites passively waiting for bites. They also cast their lures around social media, offering friend requests on Facebook, Tweeting admiringly, and so on. Their objective is usually to fake romantic interest, engage the victim emotionally, and then pretend to have some sort of “problem” that only a generous electronic friend can solve with money.

For more information on Phishing, see Phishing: Are You Protected? and Spear Phishing and Internet Security

Patriotism is another emotion to which catphish appeal. A Colorado mother-daughter team conned over 350 people by posing as American soldiers in Afghanistan. Their phishing holes were dating sites because that is where all the lonely people come. They sucked up over $1 million worth of “the kindness of strangers” before they were caught.

How to Spot an Online CatPhisher

Catphish are easy to spot if your vision is unclouded by emotion. Some of their telltale traits are:

- They never are able to meet in person; they are only available online or via phone call
- They are charming, flattering, sympathetic, and chatty;

- Claim to be U.S. citizens, but are always living in distant places for “international business” or military service
- They quickly talk about love and their eagerness for a romantic relationship
- They ask for your home address in order to send you gifts
- They often have young children, another sympathy draw
- They have sudden, bizarre financial difficulties
- Also, once you help catphish financially, they will soon be back with bigger needs.

I've been in the position of watching some of these scams as a middle man, and for a while, I didn't understand what was going on. In addition to my duties at AskBobRankin, I also operate FlowersFast, an online florist service. Occasionally, I see orders from "customers" using stolen credit cards and obviously fake U.S. addresses. A quick check of their IP address typically shows they're actually in Nigeria or Russia. But the recipients are real, and the messages that the senders attach to the bouquets speak of undying love. Sometimes these scammers unwittingly provide enough information, that I can find their profiles on sketchy dating sites.

If you say you don’t have any money, a catphish may find someone else to send you a money order, asking you to cash it and wire the money. Invariably, the money order is counterfeit and you end up losing cash.

Of course, the Internet is just a new medium for this old scam, and “catphishing” is just a new term for this type of fraud. Still, it persists because there are always people on whom it works. Don’t be one of those.

Read more: http://askbobrankin.com/are_you_a_victim_of_catphishing.html#ixzz2aSKPLsvT

Power Up Your Gmail!

From “askbobrankin.com”

Don't be afraid of that little gear on your Gmail screen... you can use it to organize your inbox, reduce the time you spend reading junk mail, and customize Gmail to work in ways that make your life easier. Read on to look at some of the fun and useful settings you can customize. I'm sure you'll learn something to make your Gmail experience even better!

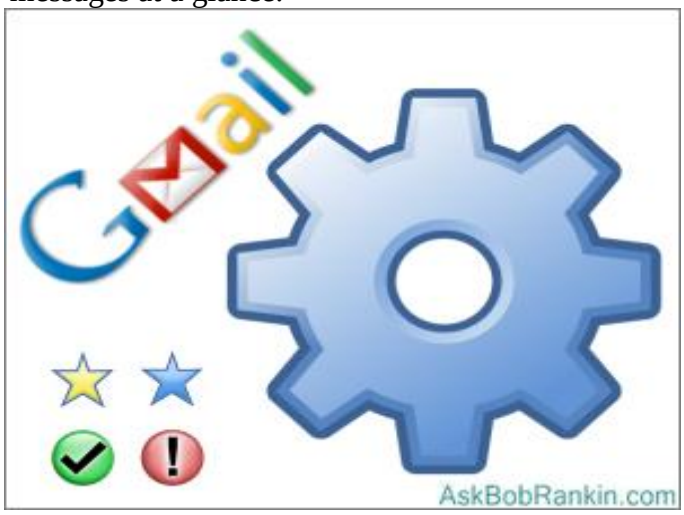
Customizing Gmail: A Quick Tour of the Settings

I started using Gmail back in 2004, and over the years, I've shared lots of tips and updates on the evolution of Google's Gmail. This article peeks inside that little gear-shaped icon in the

upper-right corner of your Gmail interface. Are you ready to teach your email some new tricks? Let's get started by clicking the gear icon, and then clicking on Settings. Then we'll explore the most useful settings on each tab.

General Tab

Maximum Page Size: Sets the maximum number of contacts or conversations (message threads) that will be displayed; handy for smaller screens or slow connections. Defaults are 50 conversations or 250 contacts. I have a large monitor and like to minimize clicks, so I max out my inbox to show 100 messages at a glance.



Browser Connection: Make sure it's set to "always use https" so that your Internet connection to Gmail is encrypted and secure from all but the most sophisticated eavesdroppers. (See The Big Problem With Wifi Hotspots to learn why this is important.)

Default reply behavior: Set this to "reply" and not "reply all." Then your boss won't get your snide remark that was intended for only one person on his mailing list.

Stars: Colorful, eye-catching labels for messages. The default assortment is one yellow star, but you can add more star types and colors; just keep clicking on the star in a message header to rotate through your available options. Some of the "stars" are actually squares, but they all work the same. I like to use the purple "?" and the red "!" to flag items as questions to be answered, or of high importance. Stars can also be search criteria, e. g., "has:yellow-star" or "has:red-bang".

Desktop notifications: When enabled, this option puts popup alerts on your PC's desktop whenever a new email or chat message arrives, so you don't have to keep checking your browser. Note: this option is for Chrome browser users only, and you must be signed into Gmail in Chrome.

Signature: Create a signature that will appear at the bottom of emails you create, and can also be inserted into replies, to indicate quoted text that was written by you.

Snippets: The first few words of a message, similar to the snippets displayed in Google Search or Google News. Turn snippets off to see just the subject lines of messages.

Vacation responder: Write a message that will be sent in response to all incoming messages, telling people you're not available and (optionally) when you will return or who to contact in your absence. If one person sends multiple messages while you're gone, the vacation response will be sent no more often than once in 4 days. The downside is that you're alerting the world that you're not home, and your house is guarded only by goldfish. With the ability to check email on mobile devices, I feel that the vacation responder is less useful now than in the past.

Inbox Tab

Inbox type: Select "priority inbox" and unread messages and messages marked "important" will be displayed first, followed by starred (read) messages and then everything else.

Select "default" inbox type and you'll see Google's latest innovation: up to five Categories of mail (Primary/general; Social media such as Facebook notifications; Promotions from Groupon and other marketers; Updates including e-bills, bank statements, etc.; and messages from Forums to which you may belong. Categories appear as tabs on your inbox page. Turn off all Categories to display everything in your inbox the traditional way.

The trouble I see with Categories is that an "unread messages count" is displayed only on the Primary tab. You get no prompts about unread Social, Promotions, etc., messages, so you must remember to check those tabs occasionally or you may miss some things.

Accounts Tab

Send Mail As: edit this option to send new messages and replies from any of several email accounts you may own. This gives you the ability to change the "From:" line in your outgoing messages.

Check mail from other accounts (using POP3): Gmail can pull email from up to 5 other email accounts you own, even if they're not Gmail accounts, and display all your mail in Gmail.

Grant access to account: Specify trusted Gmail users who can read and send email on your behalf. Good for delegating email management at work or while you are out of touch. Also good for accidentally granting access to your ex-girlfriend. Be careful with this one.

Filters Tab

Gmail filters are powerful tools for sorting and tagging, filing, deleting, forwarding, and otherwise managing incoming email automatically. For some bizarre reason, the "create new filter" link is at the bottom of this tab page instead of at the top where it belongs. Read

about the rich tools available in filters here.
(http://askbobrankin.com/gmail_spam_filter_settings.html)

Forwarding Tab

Add an address to which incoming Gmail messages will be forwarded automatically. Specify whether the original message should remain in your Gmail inbox, be deleted, or be archived after a copy is forwarded. (Alternatively, create filters that forward messages that match specified criteria).

Labs Tab

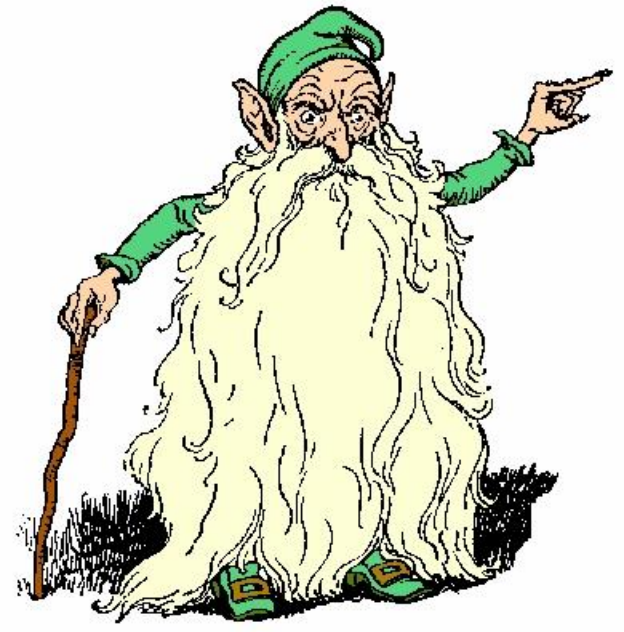
This tab is a playground and showcase for Gmail features that are still in development. I wrote a whole article about some of the fun things you can try in Labs.
(http://askbobrankin.com/gmail_on_steroids.html)

The gear icon on your Gmail page is easy to ignore; most of the time, for most people, Gmail just works. But you should familiarize yourself with these and other settings options. If you use Yahoo Mail or Outlook.com (the replacement for Hotmail), you can probably find some similar settings and customization options there. Explore and experiment!

Your thoughts on this topic are welcome. Post your comment or question below...

Read more: http://askbobrankin.com/power_up_your_gmail.html#ixzz2aSWUrNIQ

Most Mobile Apps 'Leak' User Data, Report Says



By John Lister on 20130802 in "infopackets.com"

A newly-published report says that more than four in five of the most popular smartphone and tablet applications put users' personal data at risk. The problem: these apps send critical user information to app developers.

The study comes to us from Appthority, a company that specializes in monitoring mobile applications. It looked at 400 apps, including 100 of the most-purchased and 100 of the most-downloaded apps for iOS and Android. (Source: appthority.com)

Overall, the firm found that 83 per cent of apps (including 93 per cent of free apps and 78 per cent of paid apps) displayed "risky behavior". By system, the problems affected 91 per cent of iOS apps compared with 80 per cent of Android apps. (Source: eweek.com)

One limitation to these figures is that they cover seven different types of risk, which vary in severity.

The two least-common risks were among the most potentially harmful, including a) the app accessing the user's calendar (done by 8 per cent of paid apps and 15 per cent of free apps), and b) the app accessing the user's address book or contact list (21 per cent paid / 42 per cent free).

Most Paid Apps Track User Location

The most common problem involved an app tracking and sharing a user's personal details. For example, 41 per cent of free apps and 77 per cent of paid apps tracked a user's physical location.

Other data-sharing problems involved an app passing on personal details to advertising networks (28 per cent paid / 51 per cent free).

"Single Sign On" Feature Could Increase Dangers

The other two problems involved very different types of risk. For example, 37 per cent of paid apps and 61 per cent of free apps allowed a user to sign in to a service on a computer and then automatically access the same service through a mobile app without signing in again -- something that could be risky if somebody hacked or stole the device.

Meanwhile, 42 per cent of free apps and 50 per cent of paid apps used some form of in-app purchasing. Appthority didn't clearly explain why this was a security risk.

Whether such data sharing is a problem depends on three specific factors: 1) Whether the user is aware the data is being shared; 2) Whether the app developer can be trusted with the data; and 3) Whether both the app and the phone system are secure enough to prevent the data from being stolen or hijacked by a third party.

SAFE MODE! Why do I need Safe Mode in Windows 8?

This great question recently made its way to us from a frequent Infopackets reader:

"Hi guys, I just purchased a Windows 8 PC. For the most part I'm enjoying the new OS. However, I noticed that Safe Mode is no longer available. I think this is an important feature and can't figure out why it would have been removed. Is there a way to bring it back?

Thanks!
Richard F."

Yes, Richard, it is an important feature. There are many situations in which it's helpful to boot your computer into Safe Mode. So it's good to know you can do this in Windows 8. Actually, there are two ways to access Safe Mode in Windows 8.

First, you can access Safe Mode after reaching the Windows 8 desktop in Normal Mode. However, in situations where a problem prevents a normal boot up, that won't work. You'll need to access Safe Mode the second way: from Windows 8's Recovery Console.

Running Safe Mode in Windows 8

To access Safe Mode from the desktop after a normal boot, press Win + R to access the run dialog. Then enter the command 'msconfig' (no quotations).

In the Boot tab, check Safe Boot and select the desired type of Safe Mode (several options are available). Now click Apply and reboot your machine to have it boot into Safe Mode. (Source: about.com)

Running Safe Mode When Windows 8 Will Not Run Normally

To access Safe Mode in Windows 8 when Normal Mode cannot be accessed, hold down the Shift key and repeatedly strike the F8 key as the system is trying to boot up. This will open Windows 8's helpful Recovery Mode.

With the Recovery screen displayed, click on the 'See Advanced Repair Options' button.

At the next screen, hit the Troubleshoot button and then click 'Advanced Options'. This is where you can access 'Windows Startup Settings.'

This will lead to a screen asking you to restart the computer. After it restarts, you will be greeted with the familiar Advanced Boot Option screen (the same one that has been available since Windows XP).

From this screen, you can select Safe Mode, which allows you to access the Windows 8 desktop with the usual precautions in place. (Source: redmondpie.com)

These same steps can be followed to return Windows 8 to Normal Mode. After entering the Windows Recovery Mode, simply uncheck the Safe Boot option. When the machine restarts, Windows 8 will return to Normal Mode (so long as that's technically possible).

A computer once beat me at chess, but it was no match for me at kickboxing.
~ Emo Philips.

Child spends £4,000 in-app on iPad horse game

THAT'S over $6400 U.S.

Another one
By **Dave Neal**
Thu Jul 18 2013, 09:44

A MAN IS MAD because his young daughter used his iPad to spend his money on virtual tat for an iPad game called *My Horse*.

We've heard of this sort of thing before, and consider it unwise to use Apple's or anyone else's gadgets as child minders, but it does seem to keep happening.

All we can recommend is that anyone with a child, not enough time to engage with them, and an iPad should consider looking at Apple's guidance for setting up parental controls and spending restrictions. That would seem, at least to an outsider, the best way to avoid having a child spend all your money on rainbow bangles and unicorn treats.
In the latest story, which we find on shock news website the Daily Mail, we meet a chap called Lee Neale, 43, his sad face and the aforementioned *My Horse* game.

Neale's daughter, 8, managed to run up a bill of £4,000 on virtual horse tack and tat in a five month period after she clocked his password and used it repeatedly.

The first Neale knew about it was when the money came out of his bank account and locked him out of spending anything on anything, including cyber saddles.

"Lily is only eight and hasn't grasped the concept of money. She probably wouldn't know how much a bag of crisps costs," howled Neale.

"I was very surprised how dismissive Apple were. This was an eight-year-old girl. Basically iTunes have told me categorically that I won't be getting my money back. I am also disappointed that my bank didn't alert me to what was going on."

Neale, who is an aerospace engineer, suffered because the email notifications that he was getting about his, rather his daughter's, spending were going to a work email account that he didn't have access to at the time. He's not happy and thinks that people should be made more aware of free games that require in-app real money purchases to actually do anything.

"I just think these in-app purchases are terrible and people need to be aware," he said.

And last but not least:

FREE: Encryption Tools to Protect Your Data

Category: Email , Privacy , Social-Networking

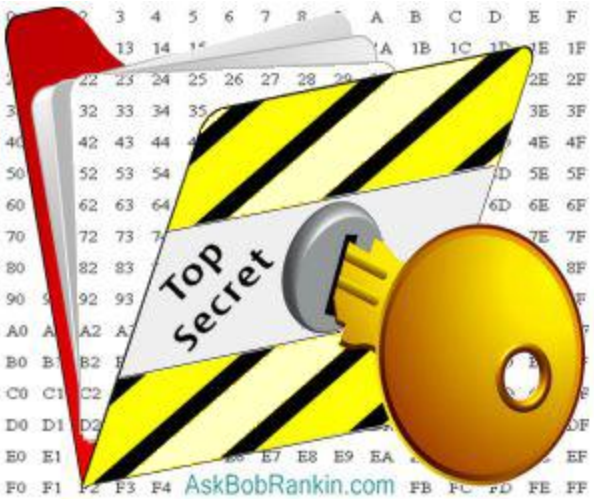
With the U.S. government ignoring the 4th Amendment, data breaches in the news every week, and identity thieves everywhere, more and more people are wondering how to protect their data and personal information. The answer is encryption, and it's no longer rocket science. Here's what you need to know about using encryption...

Use Encryption to Protect Your Privacy

Encryption is the last barrier between your personal business and other people's noses. The good news is that free, high-security encryption tools are widely available, and they're easier to use than ever. But it does take a bit of extra effort to make them part of your secure communications and data storage.

With the government snooping into our phone records, emails and who knows what else, it may be time to trade some convenience for greater security.

I have written about encrypting local hard drives and removable storage media with free software such as TrueCrypt and SafeHouse Explorer. These solutions protect locally attached storage devices that you can lay your hands on.



But lots of data resides in the cloud now, passing through and being stored on other people's servers. Most service providers do not encrypt users' data and even if they do, they can be compelled to turn over decrypted copies to government agencies. Thanks to so-called "National Security Letters," your trusted service providers cannot even tell you that they have been ordered to surrender your data. See my related article Is Cloud Storage Secure? to learn more about securing the data you store online.

Your only defense is to encrypt your data in such a way that intermediaries cannot decrypt. That means encrypting your files BEFORE they travel over the Internet to cloud storage.

Government surveillance aside, service providers themselves may mine stored copies of your data for profit. Ads on user interfaces and offers received via email or social media feeds are tailored to your inferred interests by analyzing the content of emails, Tweets, Facebook posts, your web browsing history, and other stored data. If your data is encrypted, it can't be analyzed.

Of course, that doesn't mean you will get less spam or online ads; it just won't be as creepily related to your online activity. So the choice boils down to "give me ads that are completely irrelevant and/or offensive" or "give me ads that are (sometimes) related to what I do online."

Encrypting Your Email

Email can be encrypted before it is sent so that messages stored on mail servers cannot be read. Microsoft Outlook has a well-hidden encryption feature that can encrypt individual messages or every message sent. Mozilla Thunderbird can encrypt email with the aid of addons such as GPG and Enigmail (https://support.mozillamessaging.com/en-US/kb/digitally-signing-and-encrypting-messages). But many people rely on Webmail rather than desktop email clients. A number of encryption solutions are available for them.

EncryptFree works much like an online translator. Write your message text. Copy and paste it into Infoencrypt's online form. Enter a password of your choosing and click "Encrypt." Copy the encrypted text generated by EncryptFree into your email form and send it. Communicate the password to the recipient by some means other than email. The recipient can use the password and Infoencrypt to decrypt your message. Yes, it's a hassle, but it works with any email app. (I personally prefer to send the lid of a Snapple bottle by carrier pigeon, with the understanding that the message inscribed on the underside is our secret decryption password. Shhh, don't tell the NSA...)

If you're a Gmail user, SafeGmail is a free extension for the Chrome browser that encrypts and decrypts Google Mail messages on the sending and receiving ends. Mail is encrypted during transit and while it resides on Gmail's servers.

Hushmail has been around since 1999, providing end-to-end encryption of email. It supports mobile platforms including Android, Blackberry, and iOS.

Encrypting Your Social Media Postings

Twitter, Facebook, Google+ and other social media posts can be encrypted using Scrambls. A browser plugin encrypts selected text before it is posted to the service. Unauthorized viewers see only garbage text.

Abine has an app that encrypts Facebook chats. The Encrypt Facebook extension for Chrome browsers enables secure Facebook groups.

Make sure the encryption tools you use employ the strongest possible encryption, or your data could be unscrambled by a teenager with a spare PC and time on his hands. Currently, AES 256-bit encryption is the standard to look for.

Read more:
http://askbobrankin.com/free_encryption_tools_to_protect_your_data.html#ixzz2YGtx8T96