

# Blu



**BEWARE OF CYBER CRIMINALS**

Just like a bad part of town where you keep your hand on your wallet or clutch your handbag, internet users need to beware of cyber criminals who lurk on dark side roads of the information highway trolling via unsolicited e-mails for unsuspecting victims.

# ffing Aid

By James Hutchison

## Development organizations are battling scammers on the internet who usurp their organizations' names and programs to offer bogus jobs and grants... for a price

**G**lobal Builder Sandra J. has an interesting offer for you. Not only does she promise work with the Asian Development Bank's (ADB) Water for All program in her e-mail message, but she also says you can do it from home. The best part is that you will get paid every 2 weeks! You have to agree with Sandra: opportunities like this don't come by every day. This is no get-rich-quick scheme, she assures, and it must be genuine, because her e-mail includes a link to ADB's website.

As generous as Sandra's offer is, you might want to consider an even better e-mail offer of a six-figure salary as an environmental officer with the World Health Organization.

But does a job like that make sense when you can have your very own development grant, supported by the African Development Bank, the United Nations (UN), the World Bank, and even the European Commission?

Keep all this mum as the West African gentleman involved insists the matter remain strictly confidential. But really, why bother with grants and jobs when he is willing to pay a couple of million dollars for your help? It seems he is having a terrible time trying to move a few million out of an African Development Bank account and just needs your bank account details and some paltry processing fees to get the job done.

If that sounds illegal, you might want to take advantage of another amazing e-mail deal from the UN and the World Bank. At a closed meeting, these two development

a website supported by the US Federal Bureau of Investigation or FBI ([www.lookstoogoodtobetrue.com](http://www.lookstoogoodtobetrue.com)) are sad stories of people like Jackie. Contacted by someone in

West Africa regarding a bank draft for \$400,000, she sent the required \$200 service fee plus insurance for the draft of \$1,000 only to be told the draft had been seized by a money-laundering squad. She sent another \$4,000 to get it back. Then the crooks strung her along for more fees, document stamps, and taxes totaling over \$11,000. When a further \$11,000 was requested, she and her friends investigated. She was devastated to realize she had lost over \$16,000 to a classic internet advance fee fraud, one of the most lucrative, cruel, and least prosecuted of cybercrimes.

Just like a bad part of town where you keep your hand on your wallet or clutch your handbag, internet users need to beware of cyber criminals lurking on dark side roads of

the information highway who troll via unsolicited e-mails for unsuspecting victims. Advance fee scams that trick internet users into sending money for promises of cash, jobs, free trips, and lottery winnings are almost as old as the internet and, before that, were perpetrated by letter, phone, and fax. One version known as "The Spanish Prisoner" is thought to date from as far back as the 16th century and bares a remarkable similarity to scams reinvented in digital form that caught Jackie.



**“Although there is no financial loss to the bank, these crimes impact our reputation and image.”**

—William Godbout  
Chief Security Officer  
African Development Bank



organizations have approved a contract payment in your name for \$8.3 million. Who knew the World Bank and the UN gave away that kind of money? And all they need is your banking information!

### Money for Nothing

Every year, thousands of internet users hit "reply" instead of "delete" or follow links in such unsolicited e-mails and wind up scammed out of millions. Posted on

The best known internet scam is the Nigerian Letter or 419 scam, the number relating to the Nigerian criminal code that the fraud violates. This type of fraud is famously perpetrated by Nigerian scam artists on a near industrial scale. But like all internet crimes, it transcends borders and can originate in newly evolved forms from the Russian Federation to the Philippines. Scammers are innovative and constantly changing. They use convincing pitches featuring official-looking e-mails purportedly representing a foreign government or agency to con victims. Once hooked, they are so desperate to recoup their losses, they keep sending money in the hope that the false promises will turn out to be real.

A recent twist is the fraudulent use of development organizations to add authenticity to hoaxes, some featuring cloned websites, stolen official letterheads, and logos as well as the names of real senior officials. The World Bank, International Monetary Fund, UN, and ADB are just a few targeted by online scammers. All post alerts on their websites with links for reporting scams.

William Godbout, chief security officer at the African Development Bank, reported an exponential increase in the volume of online criminal activity using the bank's trademark at the 6th German Anti Spam Summit in October 2008. "Although there is no financial loss to the bank, these crimes impact our reputation and image," he says.

Cheeky scam artists are even using the names of Interpol and the FBI to snare victims. Internet experts at Microsoft say the growing problem of internet scams not only undermines the image of legitimate organizations but also damages the credibility of the internet itself as a trustworthy source of information and commerce.

At the same summit, Tim Cranton of Microsoft's Worldwide Internet Safety Programs noted that scams can be so creative and plausible that internet users simply do not know who they can believe. Commenting on a recent rise in advance fee fraud scams promising lottery win-

nings, he says: "Lottery scammers prey not on software but on the hope of their victims." Although some of the scam e-mails are crude, littered with spelling and grammatical errors, and are from free e-mail accounts such as Yahoo! instead of a domain and website that match the organization's name, others are so clever and slickly produced that it is hard to tell that they are not genuine.



**AS UNLIKELY AS A DOWNPOUR OF MONEY** Scam artists weave elaborate get-rich-quick schemes, promising their victims easy money in exchange for their banking information.

An independent survey of European internet users, commissioned by Microsoft in 2008, showed that 1 in 44 had lost money to internet fraud in the last 12 months. Over half of the 4,930 people interviewed said internet scams made them more reluctant to purchase goods online, with 36% more reluctant to use the internet.

#### A Dubious Invitation

One development e-mail scam in circulation mas-querades as an invitation to a confer-ence. Successful applicants

are informed their travel will be paid for but that they must pay additional costs and expenses up front. After payment, the money and the conference vanish.

Especially vulnerable to e-mail scammers are those facing a tough financial situation. With the global recession putting millions out of work, there has been a surge in scammers setting their sights on exploiting job seekers, a trend showing up in fraudulent schemes promising jobs at development organizations for an advance fee.

Also thought to be increasing because of the economic downturn is a spike in "phishing" attempts, whereby internet users are unwittingly directed via spam e-mail to malicious websites posing as legitimate organizations or companies where they provide sensitive bank and personal information. Such sites can also install malware on their computers. Another common way to steal information such as passwords and account details on phoney websites is through requests to update billing or membership information. Criminals then empty victim's accounts or purchase goods on stolen credit card numbers.

Canadian cyber cops who specialize in fighting internet crime estimate that less than 10% of internet users who are scammed report such crimes because of embarrassment. Crime does pay on the internet, and it is cheap: all criminals need is an online connection, a computer, and lists of e-mail addresses to spam hundreds of thousands of accounts. If they snare just one in a thousand, they reap huge profits. It is no mystery why cyber fraud is booming with billions of dollars being stolen from internet users and near-zero chance of thieves being caught due to the anonymous and borderless nature of the internet. The amount of fraud in each case is too small to trigger an international investigation so criminals have little to fear.

And for development organizations that have their name used in such scams, the e-mails that go out are thousands of tiny cuts in their reputations. ●

# Fighting Back

The key to defeating cyber criminals is educating internet users

Jupiterimages

With varying national jurisdictions, law enforcement, and resources between countries, it is difficult to create a single global organization dedicated to cybercrime. The Council of Europe's Convention on Cybercrime, which came into effect on 1 July 2004, was the first international treaty to attempt to harmonize national laws, improve investigative techniques, and increase cooperation among the 28 nations that signed the treaty.

A growing number of government organizations, affected industries, and law enforcement agencies are forming alliances to shut down online criminals.

In an effort to combat fraudsters who counterfeit trusted brands, the African Development Bank announced in October 2008 the formation of the Advance Fee Fraud Coalition with Microsoft, Yahoo! Inc, and Western Union Company with the goal of raising global awareness among internet users of the threat posed by hoax e-mails.

Since development organizations are not directly involved in the fraud—they are simply having their names hijacked—the key to defeating the cyber crooks is educating internet users to better protect themselves against fraudulent activity.

Organized online vigilantes sites such

as 419 Eater ([www.419eater.com](http://www.419eater.com)) invite internet users to the cybersport of scam baiting—fighting back and having fun turning the tables on internet criminals. The goal of scam baiting is not only to string scammers along and waste their time and money but to get them to stand in front of a web camera holding ridiculous signs or appearing in outrageous poses. In these counter-scam operations, the often-humiliating and hilarious pictures and videos of online crooks are posted on the site's Trophy Room.

Experts agree that cyber fraud is not going away anytime soon, and the best way to defend against it is awareness. The best tool against online criminals is to use the delete button when you receive unsolicited e-mail "offers." If you do not communicate with crooks, they cannot scam you. Spam and junk mail filters help reduce the number of unsolicited emails.

Ensure you are using a secure website when submitting personal or financial details. Check to make sure the lock icon is showing on your browser that indicates your information is secure during transmission. Do not click on links on an e-mail message, text, pop-up, or instant message, and never open unexpected attachments that may contain viruses, malware, and other executable programs designed to steal information or perpetrate other

crimes. Microsoft advises users to update and install the latest security updates and turn on the automatic update feature.

On the information highway, skepticism is your best friend: if it sounds too good to be true, it probably is. Should you not be suspicious of a request for up-front money or that the United Nations or the World Bank is so delighted to be offering you great jobs or invitations to meetings?

Real organizations give their employees internal e-mail addresses. They do not use free ones such as Yahoo, MSN, or even Google. Be suspicious of e-mails asking for personal information, particularly bank or credit card account numbers, passwords, or personal identification numbers, or e-mails requesting you to update billing or membership information. When in doubt, contact the company directly by phone to confirm the correspondence. Do not fall for e-mail scammers who use your real family name to inform you of an "inheritance" or the like from a long lost relative. It is surprisingly easy to find surnames on the internet.

Almost all development organizations have a contact on their websites where you can report e-mails misusing their domain names. Reporting e-mail scammers helps stop fraud by alerting others and allowing organizations to pass details onto authorities. ●