

## Crime Prevention News

November 2009 - Page 1



### "Smishing" Emerging As New Threat To Cell Phone Users



Smishing is a new term derived from the combination of SMS (Short Message Service) and phishing, is the latest form of social engineering targeting consumers. It uses mobile devices like cell phones or PDAs to entice recipients to call a telephone number or visit a Website and provide personal or account information. With many banks today offering mobile alerts to it's customers, thieves are using this technology to trick users into divulging their information.

These scams typically start as a mass text message purporting to be from a business that retains customer accounts, such as your financial institution, e-Bay or Amazon. The messages typically claim that the recipient's account has been temporarily locked and the receiver must call a telephone number or visit a Website to unlock it. Of course, the telephone number and Website require the submission of account or personal information to unlock the account.

While the primary goal of these types of scams is similar to the other types of social engineering scams, the most dangerous threat posed by smishing is the relatively unsecured nature of cellular telephones and mobile technology. Unfortunately, as cellular telephones get "smarter" or more akin to small portable computers, the security features of many of the wireless connections have not kept pace. This provides the perfect opportunity for cyber criminals to defraud account holders.

Since this is still an emerging technology, many cellular providers and security agencies are developing fraud prevention measures to protect consumers. As you shop around for new "smart" telephones, pay close attention to the security features these telephones can offer. If you believe you have received a smishing message, do **not** call the number provided or visit the Web site indicated. Immediately contact your financial institution and request an increase in your account monitoring and watch for unauthorized purchases. Many cellular carriers offer contact information to report incidents of fraud scams. Check with your cellular carrier to see about their reporting policies.

If the message directs you to call a telephone number or visit a Website, you can file a complaint with the [Internet Crime Complaint Center](#) (IC3), a partnership of the Federal Bureau of Investigation (FBI), the National White Collar Crime Center (NW3C), and the Bureau of Justice Assistance (BJA), which receives, develops, and refers cyber crime information to alert the appropriate authorities of suspected criminal or civil violations.

**REMEMBER:** No bank, financial institution, e-Bay, Pay Pal, etc., will ever send you a message asking you for your personal information. If you are unsure, call your bank at the number on your ATM / Credit card, or statement and inform them of the message.



### A Robbery Recidivist Apprehended thanks to Public Safety's Campus Watch Program

Thanks to Public Safety's Campus Watch program, a Campus Watcher on his way home observed a robbery in progress at the 96th Street & Broadway Subway station. Keeping a safe distance, the Campus Watcher immediately called 911 giving the dispatcher a description and the direction of the flight of the perpetrator, who had ran into a nearby supermarket to hide. He was apprehended immediately by the NYPD, the victim was unharmed. The robber, who has a long history of committing robberies, could not figure out how he was apprehended so quickly!

The Public Safety Campus Watch program has been a big success since it's inception, assisting the NYPD and Public Safety by reporting suspicious activity or crimes in progress in the community. The Campus Watch program is a volunteer program. Campus Watchers receive free training and anonymous ID numbers to call the Police / Public Safety. For more information on Campus Watch, please call our Crime Prevention office **212-854-8513**.

## Crime Prevention News

November 2009 - Page 2



### Bike Theft Incidents on the Rise: Join Public Safety's Free Bike Registration / Discount Bike Lock Programs

According to a survey done by the New York City Transportation Alternatives organization, bike ownership has increase dramatically. This is great news for the environment, public and individual health. Unfortunately, we've also seen an increase in reports of bike theft. Already labeled the "bike theft capital" of the nation, the number of these crimes in New York City has increased. A major cause is the improper securing of bikes. In each bike theft report received by Public Safety, the owner had used a cable type lock to secure their bike, or had not properly secured it. Public Safety offers **FREE** bike registration by appointment with the NYPD / CU, as well as discounted Kryptonite bike locks. Please avoid using any type of cable type lock, they can easily be cut. Always use a U-shape type lock and secure the frame and tire together to a bolted down bike rack, not to **STAIRWELLS** or **HAND RAILINGS**. For more information please call **212-854-8513**.



### Lost Books and Memory Sticks: Number One Items in Lost & Found



Public Safety is the central location for Columbia University's Lost & Found. Typical items found on campus include books, memory sticks, clothing, cell phones, calculators, and other small electronics. These items are turned into Public Safety, where they are logged & stored. A big effort is made to reunite each lost item with its owner. However, we noticed that the majority of books and memory sticks we receive do not have any owner information, making it difficult to return. Not only are these text books expensive, notebooks with important class notes are lost as well. We strongly recommend the following:

- Write your name and an "**If Found**" contact in the beginning and end of your book.
- Mark your memory stick with a permanent marker with your name or even your UNI (University Network Id) on the outside.
- Set up an "**If Found**" document in your memory stick listing your contact information or an e-mail address.
- Add an "**If Found**" contact in your cell phone with an alternate contact number for yourself.

**Public Safety Lost & Found locations:** Morningside Campus– Low Library room 111 Phone # 212-854-2797  
Medical Center Campus– Black Bldg room 109 Phone # 212-305-8100



### Need a Laptop Lock? Check out Public Safety's Discount Laptop Lock Program

CU Public Safety offers Kensington Ultra laptop locks, rated number one laptop lock by Consumer's Reports. Locks can be purchased at **discounted prices** from the following Public Safety locations:

Morningside Campus– Low Library room 111 (9am-5pm Mon-Fri)  
Medical Center Campus– Black Bldg, 650 West 168 Street room 109 (24 hrs)

Please avoid using "**COMBINATION**" type locks, which jam very easily and cannot open. Department accounts are welcomed. For more information please call **212-854-8513**.