Two Emerging Scams

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

I recently learned of a two scams that everyone should know about.

Just to remind readers about the 4-1-9 scam (named for the laws in Nigeria that cover such frauds), the trick works by offering some dupe a portion of large sums of ill-gotten gains as a fee for participating in a money-laundering operation. Millions of dollars of currency are to be placed in the dupe's bank account; when the deposits have cleared, the dupe is to send most of the money back to the criminals, keeping millions for himself or herself. The criminals always make it clear in their spam that they have acquired access to funds through dishonesty (bribes, profits skimmed from mines, money embezzled from government funds); no honest person would agree to have any anything to do with such people.

In a variant of the Nigerian 4-1-9 scam reported in RISKS, a victim receives a cashier's check to deposit in a bank account in the US. After the bank informs the victim that the check has cleared, the criminals ask for part of the money to be returned to them. A few days later, the bank informs the victim that the cashier's check was a counterfeit. The money that was sent to the criminals is gone and is entirely the responsibility of the victim to replace if necessary.

Moral: don't try to get money for nothing. And don't deal with self-professed criminals.

* * *

Most readers probably know that e-gambling and e-porn sites have been implicated in fraudulent credit-card charges -- especially off-shore operations not subject to US jurisdiction.

In recent correspondence with a reader, I have learned of a new wrinkle: brazen demands for payment by pornography sites.

The reader wrote to me describing what appears to be a fraudulent demand for payment for alleged access to a porn site. The caller claimed that had provided pornography "to this computer" on a specific day. It turns out that my reader, a mom laid up that day and staying at home, knows for sure that no one was even using the computer, let alone surfing for porn. The caller, who was quite offensive, told her that "the teenager" must have done it and repeated his demand for $150 -- all without the slightest shred of evidence that the reader's family had anything to do with the issue. In a typical ploy used by criminals, the caller insisted on immediate payment "or he would turn the case over to a collection agency."

I wrote back that this business sounds like a total scam. Although I am not a lawyer and this is not legal advice (for legal advice, consult an attorney), it seems to me that without some evidence of a valid contract, the reader has zero obligation to pay anything to anyone making unsubstantiated allegations. And certainly no one should ever give their credit card information to any stranger via the phone for any reason.
The most preposterous claim is that the porn merchant was able to narrow down the source of the alleged usage to "your computer." Even if he has a record of the IP address of the alleged user’s computer, how would he know the IP address of a computer in someone's house -- especially when most people using an Internet Service Provider are assigned dynamic IP addresses (they change for every session)? My bogosity alarm went off on that one too.

Finally, the whole situation sounds very fishy. I've never heard of a porn site offering porn on account: they ask for credit-card information _before_ showing naked ladies (or whatever). There have been documented cases where credit cards have been charged _after_ supposedly "free" access to naughty bits; the criminals count on victims' embarrassment to reduce claims.

I urged the reader to stand firm and to inform her local police if they have an Internet-frauds officer. She replied that she lives in Alaska but the porn merchants are in Georgia, so I suggested she contact the local FBI office to report what might be interstate wire fraud. There’s a complete list of FBI offices at <http://www.fbi.gov/contact/fo/fo.htm>.

It’s also possible that her family is the victim of identity theft; she should discuss that possibility with her FBI contact as well as with her credit-card providers and banks. In addition, there’s a wealth of resources about ID theft at <http://www.consumer.gov/idtheft/>.

But my advice remains to let them sue -- I'm sure they won't. Frausters work on percentages; if you resist, they leave you alone.

* * *

* * *

NEW! 18-month online Master of Science in Information Assurance offered by Norwich University; see <http://www3.norwich.edu/msia> for full details.


M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:mkabay@norwich.edu>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2003 M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.