by dick kaser

From the Sidelines

Occasional Observations of the Library World From a Journalist's Point of View

A Few of My Favorite Phish

INSTALL ANTIVIRUS SOFTWARE, BUT ALSO THINK BEFORE YOU CLICK.

One of the biggest security risks for all organizations operating in the digital age is employees or patrons clicking on an email link or attachment that they shouldn't. Doing this enables hackers to gain access to their login credentials, or it gives them the ability to plant viruses on the system. Although my company email goes through several virus detection systems before landing on my laptop, I've been noting this year that a number of scams still get through.

In this article, I'd like to offer some real-life examples of efforts to get me to click on bad stuff or to reveal my credentials. Perhaps you'd like to share them with your patrons.

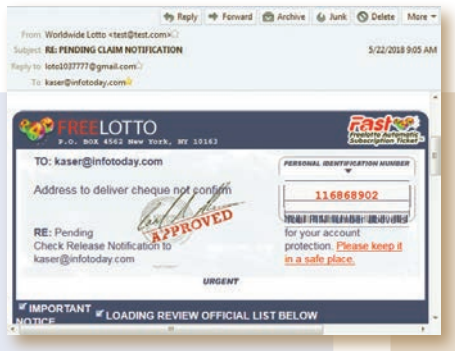
Can you spot what makes these emails clickbait?

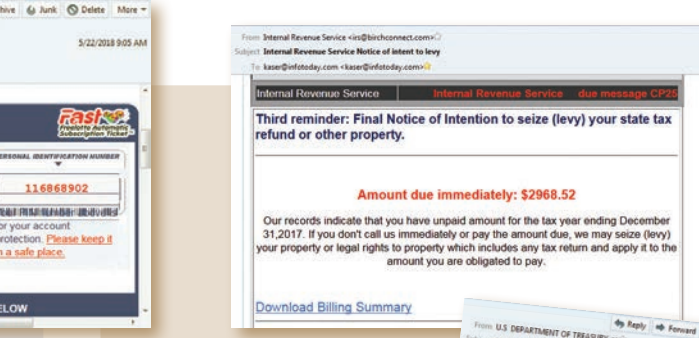
1. Lucky Me

I not only won the lotto ...

... but I'm moving to Canada.

Ancient adage: If an offer seems too good to be true, it probably is.





2. OMG

Uh oh, now the IRS is after me ...

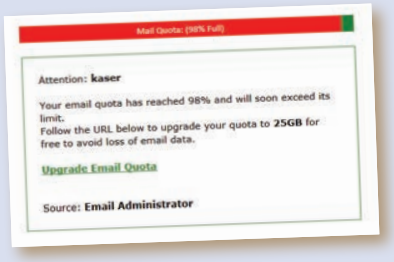
... but I won't have to worry once the Feds send me my check.

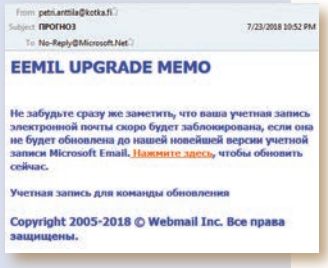
Trust me, if the IRS is after you, you'll receive a letter in the mail—and if you're due a refund, ditto.

3. Now What?

I just learned from systems admin that my email is almost full ...

... and so is my offshore account.



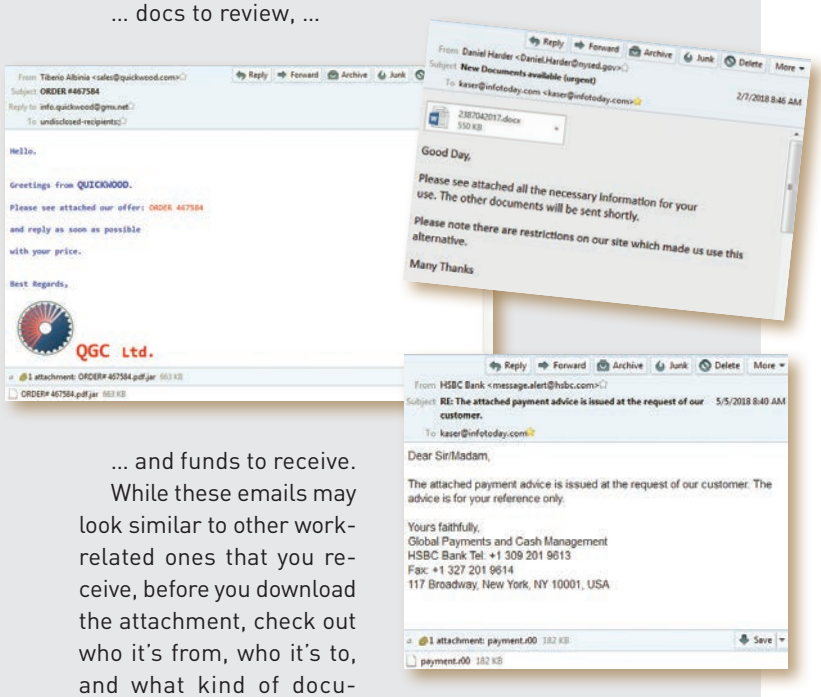


Don't click on the links in such emails. Log on to your email account as you normally do to see if there's really a problem—or contact your mail systems administrator.

4. Work, Work, Work

I've got orders to process, ...

... docs to review, ...



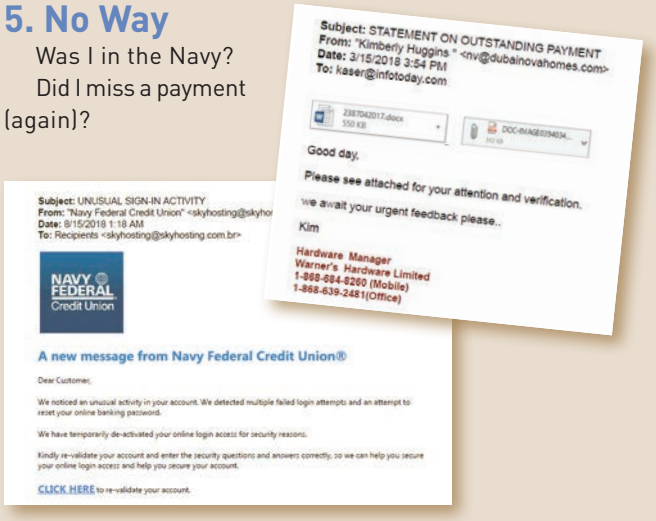
... and funds to receive.

While these emails may look similar to other work-related ones that you receive, before you download the attachment, check out who it's from, who it's to, and what kind of document is attached. A .jar file indicates it's possibly a JavaScript program that can do nasty things to your machine. R00 files are compressed archives that may contain malicious code. But even HTML, .jpg, and .pdf files can contain embedded viruses. So the acid test is whether it looks and feels legit.

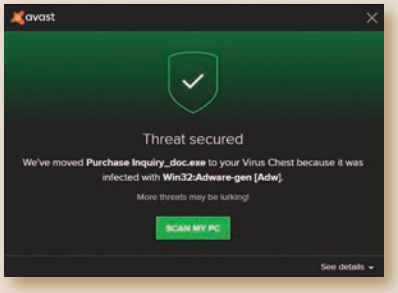
5. No Way

Was I in the Navy?

Did I miss a payment (again)?



It's easiest to spot these attempts to get your personal information if you've never done business with the company that is purportedly writing you. Just mark it as spam and delete it. Messages sent to multiple recipients and that don't use your name in the message are mostly likely bogus. The greatest irony is that many of these spammers say you've been exposed to a hacking attempt. Your bank will call you if it notices unusual activity on your account. Even then, be circumspect.



Scammers and phishers are out to get your login credentials or other personal information and/or plant malware on your computer by embedding it in attachments (or by asking you to click through to malicious websites that will do the job for them).

Install antivirus software, but also think before you click. ■

Dick Kaser (kaser@infotoday.com) is the executive editor of *Computers in Libraries*. He is an independent journalist who has been covering the information industry and library technology for more decades than he can remember.