

How to talk to patrons about: *How to Spot a Phishing Scam*

- Often, phishing scams come from email addresses that look like an official address but are not. For example, Bank of America email addresses look like this: name@department.bankofamerica.com. If you get an email from an address that looks like this: bankofamerica@gmail.com or bankofamerica@bankkofamericaa.com, this is likely a phishing attempt.
- If it looks too good to be true, it probably is.
- Never click on a link or download an attachment. If you're worried about your account, log in separately or call the company.

"Be sure to look closely at the email address that the suspicious email came from. If there are obvious misspellings or the account is a Gmail or Yahoo account, it is probably a scam."



How to Spot a Phishing Scam

Phishing is a cybercrime to obtain login credentials or financial information from victims. A person may pretend to be a legitimate organization (bank, IRS, phone company) and contact victims over the phone, email, or text message to trick them into providing sensitive information.



How to avoid being a phishing victim:

- !!! Messages often try to create a sense of urgency ("respond in the next 10 minutes!") to get you to act without thinking.
-  Offers are often "too good to be true." Trust your gut.
-  Do not download attachments from unknown senders.
-  Don't click on a link in an email or text message. On your computer, hover your mouse over the link to view the URL or manually enter the website name (e.g., bankofamerica.com).
-  When in doubt, call the organization directly and ask if the message is legitimate.

For more information, visit <https://safedata.umd.edu>