Santa Monica Public Library Library Board

BUSINESS MEETING

SEPTEMBER 8, 2018

SANTA MONICA PUBLIC LIBRARY DIGITAL RESOURCES 2017 - 2018

Digital Collections

BiblioBoard
DRAM
hoopla
OverDrive
RBdigital Magazines
Sesame Street eBooks
Tumblebooks

TOTAL CHECKOUTS: 127,197

ANNUAL EXPENDITURE:
$241,119.02

IMAGINE SANTA MONICA DIGITAL COLLECTION

Image Archives
Palisades Historical Collection
Evening Outlook, 1875-1939

TOTAL USAGE:
18,654 SESSIONS

Research Databases

TOTAL USAGE:
88,287
SESSIONS

ANNUAL EXPENDITURE:
$100,455.46

MOST USED DATABASES

Brainfuse HelpNow online tutoring
MasterFILE Complete
ReferenceUSA
Value Line
Morningstar Investment Research Center
Mango Languages

City Framework and Performance Based Budgeting

SANTA MONICA'S

PERFORMANCE MANAGEMENT PROGRAM

SaMoStat

using data to drive performance

LIBRARY STRATEGIC PLAN

SANTA MONICA PUBLIC LIBRARY

Volunteerism at the Library

Numbers: 32 Teens, 89 Adults

- Adult Literacy Volunteers
- Homework Help Volunteers
- Santa Monica Reads Book Discussion Group Leader
- Shut-In Service Volunteers
- Teen Volunteers
- Friends of the Library Volunteers (*https://smpl.org/Volunteer_at_the_Library.aspx*)

Current volunteer needs:

Bilingual Spanish/English volunteers for SMPL Homework Help at the Pico Branch, volunteers for our Shut-In Services program, Friends of the Library Bookstore volunteers

Cybersecurity

MAINTAIN VIGILANCE

The Information Services Department would like to remind City employees to remain vigilant to indicators of suspicious activity. Cybercriminals are often hoping to catch you off guard, where you might be susceptible to their creative tactics to solicit money or information from you.

This booklet includes the following tips on how to stay alert and maintain vigilance while at work and at home:

- Keep A Clean Machine
- Password-Protect Sensitive Files and Devices
- Limit the Amount of Personal Information You Share Online
- Exercise Good Mobile Security Vigilance
- Privacy is Good for Business
- Maintain Vigilance When Receiving Email

KEEP A CLEAN MACHINE

The best defenses against virus, malware and other cyber threats are to make sure all of your computers and mobile devices are equipped with:

- Antivirus software, firewalls
- Email filters, and anti-spyware.
- Ensure machines are running the latest security updates.

The Information Services Department ensures that your computer complies with the above.

PASSWORD-PROTECT SENSITIVE FILES AND DEVICES

A good strong Password is:

- Private: It is used and known by one person only
- Changed Regularly: Every 6 months
- Relevant: Use a password phrase.

Focus on positive sentences or phrases that you like to think about and are easy to remember. For example, a good password might be a phrase "knot my pencil" for example,
which you could compose as "I<n0tmyP3n$il"

- Easy to Remember: Make it something you can visualize.
- Lengthy: At least 12 characters and include a mixture of lower case letters, numbers and symbols.
- Separate work and personal accounts and make sure critical accounts have the strongest passwords.

LIMIT THE AMOUNT OF PERSONAL DATA YOU SHARE ONLINE

- Don't overshare on social networking websites.
- Keep Social Security numbers, account numbers, and passwords private, as well as specific information about yourself, such as your full name, address, birthday, and even vacation plans.
- Review privacy and security permissions.
- Be sure to review and understand the privacy and security permissions for any website or app where you share your personal information.

EXERCISE GOOD MOBILE SECURITY VIGILANCE

- Keep track of your device at all times.
- Avoid putting down your devices in public places.
- Use strong passwords, passcodes
- Only install apps that you need and make sure that you download them from a trusted source.
- Update mobile devices and applications on a regular basis.
- Beware of SMishing; receiving a text message asking you to provide personal and or financial information by clicking on a link or responding via text or phone number. When in doubt, don't respond
- Do not access or store work email or other data from The City on your personal mobile device.
- Be careful when using Wi-Fi. Many mobile devices will automatically connect to Wi-Fi networks without asking you. Disable Wi-Fi if you are not using it.

PRIVACY IS GOOD FOR BUSINESS

If you collect it, protect it! Follow reasonable security measures to protect individuals' personal information from inappropriate and unauthorized access:

- Use Strong Passwords.
- Don't leave printouts containing private information on your desk. Lock them in a drawer or shred them. It's easy for a visitor to glance at your desk and see sensitive documents.
- Always lock/log-out of your computer when you leave it.
- Remember to shut down your computer when you leave for the day.

MAINTAIN VIGILANCE WHEN RECEIVING EMAIL

You may not realize it, but you are a phishing target at work and at home. You and your devices are worth a tremendous amount of money to cyber criminals, and they will do anything they can to hack them. YOU are the most effective way to detect and stop phishing. If you identify an email you think is a phishing attack, or you are concerned you may have fallen victim to an attack, contact the Service Desk at x8386 immediately. You may also use the *Phishme* button in Outlook or O365 to report a suspected Phish.

1. Check the email addresses. If the email appears to come from a legitimate organization, but the "FROM" address is someone's personal account, such as @gmail.com or @hotmail.com, this is most likely an attack. Also, check the "TO" and "CC" fields. Is the email being sent to people you do not know or do not work with?

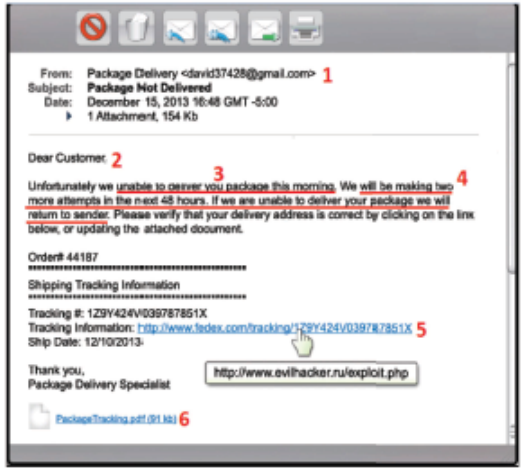
2. Be suspicious of emails addressed to "Dear Customer" or that use some other generic salutation. If a trusted organization has a need to contact you, they should know your name and information. Ask yourself, am I expecting email from this company?

3. Be suspicious of grammar or spelling mistakes; most business proofread their messages carefully before sending them.

4. Be suspicious of any email that requires "immediate actions" or creates a sense of urgency. This is a common technique to rush people into making a mistake. Legitimate organizations will not ask you for your personal information.

5. Be careful with links, and only click on those that you are expecting. Hover your mouse over the link to see the true destination of where you would go if you were to click on it. If the true destination is different than what is shown in the email, this is an indication of an attack.

6. Be suspicious of attachments. Only click on those you are expecting. Be suspicious of any message that sounds too good to be true. (No, you did not just win the lottery.) Just because you received an email from your friend does not mean they sent it. Your friend's computer may have been infected or their account may be compromised. If you get a suspicious email from a trusted friend or colleague, call them on the phone.



STAY WATCHFUL AND SPEAK UP!

• Keep an eye out for suspicious activity and if you notice strange happenings on your computer, please contact the Service Desk at x8386

Learn more about phishing at
https://www.sans.org/security-awareness-training/blog/new-security-awareness-poster-dont-get-hooked