



RESOURCE LIBRARY – SECURITY
Internet and Email Usage

CODE: 03.19.038

EDITION: 1

PAGE 1 OF 5

INTERNET & E-MAIL USAGE

网络和电子邮件的正确使用

Target Audience: All employees who use hotel computers, IT Managers

培训对象: 所有需要接触电脑的酒店员工, IT经理

Training Tip: Ask someone from the audience to share what they know about Phishing schemes. Phishing schemes are attempts by criminals to look or act like a legitimate request for personal information. Ask the audience if they have ever been deceived by a fake Web site or received a suspicious e-mail? Have them share what it looked like and what clues made them aware that the Web site or e-mail was not legitimate.

培训提示: 询问员工所了解的网络诈骗案。网络诈骗案通常是由犯罪人扮演, 并且这类人看起来像正规要求的形式来询问个人信息。询问员工是否有被假网站所欺骗或收到过可疑的电子邮件? 有分享过欺诈网站或邮件看起来是怎么样的? 又是什么让他们知道这些是欺诈邮件?

Main Content:

主要内容

This program is designed to introduce all employees in the hotel to the importance of being cautious with Internet and e-mail usage while using hotel computers.

本课程是向所有酒店员工介绍使用酒店电脑时警惕网络和电子邮件诈骗的重要性。

Many hotel employees have access to use computers while they are onsite at the hotel – whether they require access to perform their daily job functions or if there are public computers available to them to use during their breaks. Each individual should be aware of the security risks associated with Internet and e-mail usage. You can help keep your personal information and guest information secure by using caution when accessing the Internet or e-mail.

许多酒店员工都会在酒店区域时使用电脑, 不管是日常工作或是休息时都会使用到公共电脑。每个人都应该在使用网络和电子邮件时保持警惕。你可以谨慎的使用网络和电子邮件这样就可以达到保护到个人和客人信息安全的目地。

Internet Usage

网络的使用

While using the Internet, you should be cautious not to reveal personal or sensitive information online. Whether the information is yours or a guest's, the information does not need to be broadcasted to the world as it will be accessible to everyone.

使用网络的时候, 你应该很谨慎来避免透露过多的人或敏感的信息。不管这些信息是你个人的还是客人的, 都不应该把这些信息公诸于众, 让全世界的人都知道。

Not every Web site is legitimate! You should avoid unknown or suspicious Web sites and stay away from sites with potentially offensive materials. Additionally, while surfing the Web, be mindful of fake Web sites that request

your personal information – it is likely your personal information will be compromised as a result.

不是每个网站都是合法的! 你应该避免使用未知或有怀疑的网站, 并且避免带有潜在攻击性内容的网站。此外, 浏览网页时, 随时注意虚假网站所要求提供的个人信息, 不注意的结果很可能是你的个人信息被盗。

Many individuals connect to the Internet using public/shared computers. While using a computer shared amongst many users, avoid entering personal or confidential information. Sometimes this information can be saved on the computer and accessible to other users. If prompted to save a username or password, do not accept. If you inadvertently save a password to a computer, notify the IT department.

许多人会用公共电脑上网, 当使用一个许多用户都可以登录的电脑时, 避免输入个人和一些机密的信息。有时候这些信息会被保存在电脑上, 再被其他人盗用。如果电脑询问是否需要自动保存用户名或密码时, 请不要选择接受。如果你不注意同意了保存密码, 马上告知IT部门。

Internet Security

互联网安全

If your hotel offers wireless Internet, work with the vendor to ensure they set up the wireless signal with encryption. If your hotel also offers free wireless Internet in your lobby, pay attention to non-guests and report them to management.

如果酒店提供无线上网, 让供应商确保已安装无线上网密码。如果酒店在大堂提供免费无线上网, 注意不是住店客人在使用一定要及时报告给管理层。

Additionally, do not connect guest room or public wireless Internet access to the hotel's internal network and servers. If connected, tech savvy guests may be able to hack into the hotel's servers.



RESOURCE LIBRARY – SECURITY Internet and Email Usage

CODE: 03.19.038

EDITION: 1

PAGE 2 OF 5

此外，不要将酒店的内网和服务器与客房或公共无线网络相连。一旦连接上，有专业技术的客人可以破坏到酒店的服务器。

E-mail Usage **电子邮件的使用**

Use caution when opening attachments from unknown senders. An e-mail could contain malicious software disguised as an attachment which can wreak havoc on computer systems once it is clicked on.

打开未知附件的时候要特别小心。如有一个疑似的并且伪装成一个对你有用的信息附件，当你在点击此附件时，很可能会破坏电脑系统。

One way to avoid “phishing” scams is by not clicking on links in e-mails from unknown sources. These links can take you to Web sites that you were not expecting and could infect your computer. It could also be a link to a convincing fake Web site where you are prompted to type in personal information such as account user ID and password. Reputable organizations will not normally include links to your account in their e-mails. They expect you to access your account using their Web page.

防止诈骗的一个办法是不要点击未知的电子邮件链接。这些链接会强行登陆到一些你没意料到的恶意网页并且会感染你的电脑。不仅如此，这些链接还可能让你去到一个虚假网站并提示你需要填写一些个人信息，如用户名和密码。有名的网站一般不会包含有你个人账号链接的电子邮件。他们希望你使用他们的网站页面来登录。

Never enter personal or company information into a form in an e-mail or send these types of information over e-mail. E-mails can be used to trick you into providing personal information such as account or credit card information. This information could then be used to obtain goods or services in your name.

绝对不要填写个人或公司信息到电子邮件的表格里或用邮件发送这些信息。电子邮件能被用来哄骗你给出个人信息，比如账号或信用卡信息。这些信息能以你的名字来获取物资或服务。

Be suspicious of e-mails addressed to “Dear Customer” or that have numerous spelling or grammatical errors. Most official organizations will address e-mail to you personally whereas e-mails trying to falsely obtain information are normally sent to numerous people and will usually not have your name. E-mails with spelling and grammatical mistakes could indicate that the e-mail is not from a reputable source.

当电子邮件里出现“亲爱的用户”或有许多拼写甚至语法出现错误的情况发生时请一定要小心。大多数正式的网站会给你单独发邮件，反之想要非法套取信息

的电子邮件会同时给很多人发邮件并且不会出现你的名字。出现拼写和语法错误的电子邮件通常不是来源于一个可靠的资源。

Even though it could be enticing, do not forward virus warnings or chain e-mails. You don’t want to keep spreading trouble! Also, it is good practice not to respond to spam e-mails. If you reply to spam, you are confirming that your e-mail address is valid, which can encourage more spam.

尽管这些内容会有一些的吸引力，但千万不要转发病毒邮件或连锁邮件。如果你不想有传播的麻烦，那么正确的做法还包括不回复垃圾邮件。如果你回复垃圾邮件，你就证实了你的邮件地址是可用的，这样会招来更多的垃圾邮件。

For your personal safety, do not include personal or vacation details in out-of-office replies. 为了你个人的安全，不要发送个人或假期明细的回复。

Mobile Devices **移动设备**


Some individuals may be equipped with mobile e-mail devices such as BlackBerry® devices. Use caution when viewing sensitive data on mobile e-mail devices, especially when you are in a crowd. When many individuals are around you, it is very easy for them to “shoulder surf,” by looking over your shoulder and obtaining personal information they should not have.

有些人会配有移动电子邮件查看设备，比如说BlackBerry®（黑莓）。用移动电子邮件设备查看敏感信息的时候要特别小心，特别是在人多的时候。当很多人在你身边时，对他们来说盗取信息就非常容易了，通过从你的肩膀上方看过去去窃取到他们没有的个人信息。

QUIZ

测试

- When using the Internet, caution should be used not to reveal personal or sensitive information online.
使用网络的时候，你应该很谨慎来避免透露过多的个人或敏感的信息。
 - True 对
 - False 错
- Safe Internet practices include the following:
安全使用网络的习惯有以下：
 - Avoiding unknown or suspicious Web sites.
避免未知或有怀疑的网站
 - Not revealing personal information
不透露个人信息
 - Refraining from accessing Web sites with potentially offensive material.
避免登录带有潜在攻击性内容的网站
 - All of the above.
以上所有答案
- While using a public computer, you should save personal or confidential information.
使用公共电脑的时候，你应该保存个人或机密信息
 - True 对
 - False 错
- Safe e-mail practices include the following:
安全使用电子邮件的习惯有以下：
 - Opening every attachment sent to you.
打开所有发送给你的附件
 - Clicking on links in e-mails.
点击邮件中出现的链接
 - Entering personal information into a form in an e-mail.
在邮件里填写个人信息表
 - None of the above.
以上都不是
- One way to avoid “phishing” scams is by not clicking on links in e-mails from unknown sources.
防止诈骗的一个办法是不要点击未知的电子邮件链接。
 - True 对
 - False 错
- Which of the following e-mails should you be suspicious of?
下面哪些电子邮件为可疑的？
 - Those addressed to “Dear Customer.”
含有“亲爱的用户”
 - Those with spelling mistakes.
有拼写错误的
 - E-mails from unknown individuals.
来自未知发件人的
 - All of the above.
以上所有答案
- Virus warnings and chain e-mails should be forwarded:
病毒和连锁邮件应该被转发至
 - Only to hotel employees.
仅限酒店员工
 - Only when the chain e-mail is really funny.
当连锁邮件很喜剧的时候
 - Never.
绝不转发
 - To all of your friends.
所有的朋友
- You should always respond to spam indicating you want to be removed from the distribution.
你应该通过回复垃圾邮件的方式来表示你想从名单库里移除。
 - True
 - False

	RESOURCE LIBRARY – SECURITY Internet and Email Usage	<i>CODE:</i> 03.19.038
		<i>EDITION:</i> 1
		<i>PAGE</i> 4 OF 5

QUIZ ANSWERS

测试答案

1. (A) True. When using the Internet, caution should be used not to reveal personal or sensitive information online.
(A) 对。使用网络的时候，你应该很谨慎来避免透露过多的个人或敏感的信息。
2. (D) All of the above. Safe Internet practices include avoiding unknown or suspicious Web sites, not revealing personal information, and refraining from accessing Web sites with potentially offensive material.
(D) 以上所有答案。安全使用网络的习惯有避免未知或有怀疑的网站，透露个人信息，避免登录带有潜在攻击性内容的网站。
3. (B) False. While using a public computer, you should never save personal or confidential information.
(B) 错。使用公共电脑的时候，绝对不要保存个人或机密资料。
4. (D) None of the above. When dealing with e-mails, you should use caution opening attachments, never click on links in e-mails, and never enter personal information into a form in an e-mail.
(D) 以上答案都不是。
处理邮件的时候，你应该很小心地打开附件，绝不点击邮件里的链接，也不要再在邮件里填写个人信息表。
5. (A) True. One way to avoid “phishing” scams is by not clicking on links in e-mails from unknown sources.
(A) 对。防止诈骗的一个办法是不要点击未知的电子邮件链接。
6. (D) All of the above. You should be suspicious of e-mails addressed to “Dear Customer,” those with spelling mistakes, and e-mails from unknown individuals.
(D) 以上所有答案。你应该对含有“亲爱的用户”，拼写错误和未知源的邮件保持警惕。
7. (C) Virus warnings and chain e-mails should never be forwarded.
(C) 病毒和连锁邮件绝不应该被转发。
8. (B) False. You should not respond to spam indicating you want to be removed from the distribution as this will just confirm your e-mail address is valid and will encourage more spam.
(B) 错。你不能回复垃圾邮件来表明想从名字单中被移除的决定，一旦回复，就表明你的邮箱地址是可用的并会招来更多的垃圾邮件。



Checklist – Internet & E-mail Usage 检查表--- 因特网与电子邮件的使用

Internet Usage 因特网的使用

- Do not reveal personal or sensitive information online.
不要在网上透露个人或敏感信息。
- Avoid entering personal or confidential information on public/shared computers.
避免在公共电脑上输入个人或机密信息。
- Be mindful of fake Web sites requesting personal information.
警惕虚假网站的个人信息索取。
- Avoid unknown or suspicious Web sites.
避免登录未知或有怀疑性的网站。
- Do not access sites with potentially offensive materials.
不要登录有潜在攻击性内容的网站。
- Encrypt wireless signals.
无线网加密
- Do not connect guest room or public wireless Internet access to the hotel's internal network and servers.
不要将酒店的内网和服务器与客房或公共无线网相连。

E-mail Usage 电子邮件的使用

- Avoid “phishing” scams by not clicking on links in e-mails from unknown sources.
防止诈骗的一个办法是不要点击未知电子邮件的链接。
- Use caution when opening attachments from unknown senders.
打开未知附件的时候要特别小心。
- Never enter any personal or company information into a form in an e-mail.
绝对不要填写个人或公司信息到电子邮件的表格里
- Be suspicious of e-mails addressed to “Dear Customer” or that have numerous spelling or grammatical errors.
当电子邮件里出现“亲爱的用户”或有许多拼写语法错误的时候请小心。
- Do not forward virus warnings or chain e-mails.
不要转发病毒邮件或连锁邮件。
- Do not respond to spam e-mails or participate in spamming.
不要回复垃圾邮件或参与到垃圾邮件。
- Do not include personal or vacation details in out-of-office replies.
不要发送个人或假期明细的回复。
- Use caution when viewing sensitive data on BlackBerry® devices and other e-mail devices.
使用BlackBerry®（黑莓）或其他查看邮件的设备时请小心。
- Be aware of shoulder surfers who look over your shoulder to get your information.
随时注意有无他们通过你肩膀上方来获取信息。