Best Practices for Online Shopping

尽可能使用自己信任的电脑

公开可用的系统可能没有最新的防病毒软件或操作系统补丁。也可能在公开可用的电脑上安装了恶意软件或键盘记录器，用于捕获用户凭据或信用卡数据。如果您在公共场所，例如肯德基或星巴克，我们强烈建议您进行个人银行业务或网上购物，使用VPN或受信任的网络。

贝克大学的计算机定期更新。另外，我们使用软件来锁定教室的计算机配置，防止永久安装任何软件。当您启动或重新启动我们的教室计算机时，它将始终加载默认的无恶意软件的映像。

安全的浏览器连接

查看地址栏中的URL；该站点是否使用了安全连接，表示“https:”前缀？

浏览器地址

确保您在正确的网站上。虚假广告和电子邮件可能会显示看起来正确的链接，但实际上链接到不同的网站！您可以通过将鼠标悬停在链接上而不会点击来轻松检查这一点-这将在大多数浏览器的底部地址栏显示完整的URL。

例如：在浏览器中输入baker.edu并按enter键-它将在顶部地址栏显示“https://www.baker.edu”


则不是我们的安全网站。

电话和平板电脑应用程序

许多商店都有自己的手机和平板电脑应用程序。这些通常比使用浏览器更安全，因为手机和平板电脑没有光标让您在点击前看到地址。安装应用程序时，最好从商店的应用商店或制造商的网页上获得应用程序。确保从安全位置获取这些应用程序，如App Store，Google Play，或直接从制造商。永远不要从广告或电子邮件中的链接安装应用程序。
Passwords -
When shopping online, use a unique password for each site. If a site is compromised, criminals will attempt to use those credentials on other sites so never use common passwords for multiple sites. You should develop your own technique to use and remember unique passwords.

Some methods for creating strong passwords are:

- Using uppercase, lowercase, numbers, spaces and special characters.
  - (example: M4 n@m3 !5 J04n for “My name is John”)

- Using the first letter of each word in a song, phrase, or sentence, as well as using the method listed above for those words.
  - (example: !p@2Tf07U5o@ for “I pledge allegiance to the flag of the United States of America”)

Person-to-person electronic payments -
Person-to-person payments (P2P) is an online technology that allows customers to transfer funds from their bank account or credit card to another individual's account via the Internet or a mobile phone. For example, using Paypal, Western Union money orders, Square etc.

- Know your options of disputing the transaction.
- Refuse requests that avoid secure payment options.
- Test the vendor’s communication efforts.
- Research the vendor’s reviews.
- When in doubt, shop elsewhere!

Credit cards vs. debit cards -
If you typically use a debit card for online purchases, you may want to reconsider. When your card information is hacked and purchases are made without your permission, you’ll quickly find out that debit and credit cards are treated quite differently. The key difference? With a credit card, the card issuer must fight to get its money back. With a debit card, YOU must fight to get your money back. Read more here: Credit Cards vs. Debit Cards

Credit card statements -
It is a good idea to review these charges regularly to check for unauthorized charges. Most banks and credit unions have a web portal that will allow you to review charges to your card. Know your credit card issuer and become familiar with their process to review charges on your statement.
Credit card skimmers -
This technology is used to steal credit card data by attaching a device in or on a card reader at a gas pump, ATM, or similar device. When a credit card is passed through the skimmer, data on the card’s magnetic strip is recorded and saved for retrieval by the criminal. Originally, these skimmer devices were placed on the outside of the host device and often looked “out of place.” Now, criminals are using master keys to open gas pumps and are installing the skimmers internally so you can’t even see the device. When using a credit card to purchase fuel it is safest to pay inside. If you pay at the pump, try to use one of the pumps nearest (within line of site) to the business as these would be less likely to have been tampered with. For ATMs, it is always a safer option to go inside the bank whenever possible to withdraw funds. When in doubt or if something doesn’t “feel” right, try using a different device.

Antivirus and operating systems -
Don’t forget! This is a good time to check that your antivirus software and operating systems are up-to-date and patched.

Over-the-phone or online credit card transactions -
There are many do’s and don’ts for both online transactions and phone transactions. Following these few best practices might help keep your credit safe and your bank accounts stable. Remember, these ideas are only a handful of best practices to keep your financials out of the hands of Cyber Criminals. Click here to see the “Do’s and Don’ts.”