OFFICE 365 INFORMATION SECURITY Q-CARD

The following are tips for protecting your computer and the information stored on it:

Office 365 Security – Email Security

●Treat email attachments with caution. Don't click links in email messages that present business opportunities, health solutions, or discount software offers.

●Beware of email messages that tell you of winning a contest you never entered, or money you should claim, or notifies you with instructions to install software on your machine or alerts you of a billing error for a service you do not use.

●Do not use the unsubscribe function for services to which you did not subscribe since this only alerts an attacker that an active address has been located and makes you a more vulnerable target.

● Phishing e-mails are messages that are crafted to look as if they have been sent from a legitimate organization. The scam begins with an e-mail message that looks like it originates from the bank. If you click on the provided link, it steers you to a fake Website and asks you to update your security information such as account name, password and other confidential data.

●Do not respond to an email communication from an IT department that asks for your password.

Office 365 Security – File Storage

●Personal Identifiable Information (PII) should *never* be stored in OneDrive.

●Use common sense.

●Stop, Think, and Click.

●Save private document on shared drives at the office.

●Rule of thumb: Do not put any documents on One Drive that you are not going to share with others.

Email Privacy

●If you plan to send email to a group of people and want to protect their email addresses from being viewed, it is a best practice to use the "BCC:" field for all recipients. If your email client does not allow you to send a message without an address in the "To:" field, consider using your own email address in the To: field.

Password management

●Do not share your password with anyone. If someone calls and requests your password, do not provide it to them. Remember that the IT department will never call and ask for your password.

●Use complex passwords that are at least six characters in length and contain uppercase, lowercase, numbers, and special characters such as !$#.

●Use password program such as KeePass to manage your passwords.

Tips For Safe Online Banking

● Review online privacy policies and practices with your bank. Pay attention to the methods the bank uses for encrypting transactions and authenticating user information.

● Check with the bank to see if they require additional security information before they will authorize a payment to a business or individual that has never received a payment before.

● For security purposes, choose an online personal identification number (PIN) that is unique and hard to guess.

● Use a credit card to pay for online goods and services. Credit cards usually have stronger protection against personal liability than debit cards.

● When in doubt, call your bank customer service. Note: Do not call the customer service number on the e-mail message; call the number that you have on file with the bank.

● Once your sensitive data is obtained by the scammer, your account is now vulnerable for unauthorized transfers.

Clear Desk and Clear Screen

●When you step away from your desk, even for short periods of time, lock your computer by pressing "Windows Key and L " keys simultaneously to lock your desktop.

●When you are away from your desk, you need to keep your work area cleared of papers that could contain an individual's personal information.

Backup Your Data

●Make it a habit to backup your data on daily basis or at least on weekly basis. Backups can be stored on an external drive, a network file server, or a CD/DVD. It is important to have a replica of your data on another source.

●Schedule time to do housekeeping on your PC: making data backups, deleting internet browser history, and emptying the recycle bin.

Banner and Argos Security

●Do not share your Banner logon ID and password with your colleagues. If you plan to be out of office and someone else needs the same access to your Banner screen, contact your Banner Administrator to enable those screens.

●Do not leave your workstation unattended. Lock your workstation using "ctrl+alt+del" while logged on to the administrative screens.

●Do not share confidential and sensitive information such as SSN with anyone, including colleagues, unless there is a business reason.

●Ensure reports containing confidential and sensitive information are not in open area.

●When disposing reports contain confidential information, use the shredder to ensure the information is unreadable.

Incident Handling

●If you see a strange process running, or if you discover an intruder logged into your workstation, or if you notice your PC is running slow and accumulating a lot of CPU time, or if you discover a virus has infected your system, notify your IS Helpdesk or Academic Computing department immediately; these are signs of a security violation. If possible, disconnect your system from the network as soon as possible.

Keep Your Operating System and Web browser up-to-date

●Windows software patches and security updates are setup to automatically distribute to your computer. Double click the yellow exclamation icon on the task bar to start the installation.

Personal Digital Assistants (PDA)

●Enable password protection to access to your PDA data if possible.

●Synchronize contacts, notes, to do list, calendar, and your PDA settings to your desktop before long trip.

Additional Links to "Guidelines" documents

●Additional information for cloud solution security measure, click on the link below:

http://www.nocccd.edu/Departments/IS/documents/Cloud_Solution_Security_Measure_Guidelines.pdf

●CaTT Tales Archives:

http://www.nocccd.edu/CaTTTales.htm

Contact Information

● IS Help Desk: 714-808-4849

● Email: ishelpdesk@nocccd.edu

Authored by Information Services at North Orange County Community College District. Ver. 2.0