Presented by: Simar Singh
Somerset County Senior Wellness Center
August 10th, 2018
About this Course:

- Make you aware of dangers on the internet
- How to stay safe
About the Instructor:

- Cybersecurity Advanced Course - The Institute for Security, Technology and Society (ISTS), Dartmouth College - 2018
- Gencyber Basics Course - Penn State University - 2017
- Ridge Cyberpatriot Club - Captain - 2017 - present
Cybersecurity: measures taken to protect computers or computer systems against unauthorized access or attacks.
Risks on the web

- Viruses - Ransomware
- Hackers
- Spyware
- Phishing
- Online fraud
- Identity theft
How to stay safe on the web?

- Keep Your Computer Clean & Updated
- Protect your Personal Devices (Phones & tablets)
- Protect your personal information
- Email Security
- Safe online shopping
- Phishing and email scams
- Best Practices - Tips
Keep Your Computer Clean & Updated

• Update all the software and security patches
• Keep the automatic update feature ON
• Install Antivirus - keep it updated
• Keep the firewall active
• Backup your system
Update all software and security patches
Keep Your Computer Clean & Updated

- Update all the software and security patches
- Keep the automatic update ON
- Install Antivirus - keep it updated
- Keep the firewall active
- Backup your system
Recommended Antivirus

- McAfee Antivirus Plus
- Symantec Norton Antivirus
- Webroot SecureAnywhere Antivirus
- Kaspersky Internet Security
- Avast - (Free)
- Malwarebytes - (Free)
Keep Your Computer Clean & Updated

- Update all the software and security patches
- Keep the automatic update ON
- Install Antivirus - keep it updated
- Keep the firewall active
- Backup your system
Keep Firewall ON

The firewall is turned on and set up to prevent unauthorized applications, programs, and services from accepting incoming connections.

Windows Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.

Private networks
- Networks at home or work where you know and trust the people and devices on the network
- Windows Firewall state: On
- Incoming connections: Block all connections to apps that are not on the list of allowed apps
- Active private networks: Not connected
- Notification state: Notify me when Windows Firewall blocks a new app

Guest or public networks
- Networks in public places such as airports or coffee shops
- Windows Firewall state: On
- Incoming connections: Block all connections to apps that are not on the list of allowed apps
- Active public networks: None
- Notification state: Notify me when Windows Firewall blocks a new app
Keep Your Computer Clean & Updated

- Update all the software and security patches
- Keep the automatic update ON
- Install Antivirus - keep it updated
- Keep the firewall active
- Backup your system (Cloud or External Hard Drive)
Protect your personal devices (SmartPhones, tablets)

- Physically protect
- Lock with strong password
- Short screen lock time
- Set remote wipe option on
- Install Apps from secure locations - AppStore, Google Play store
  - Delete old unused apps
How to Protect Personal Information
Strong Passwords

• Should be about 10 characters
  • Make your password a sentence (“I love country music”)
• Should contain 1-3 numbers
• Contain caps and lower case
• Include different symbols (such as ; &)
• Unique account, unique password
• Keep passwords in safe place
• Don’t use personal information
  • Birthdays, last name, kids
Weak Passwords Vs. Strong Passwords

<table>
<thead>
<tr>
<th>Weak Passwords</th>
<th>Strong Passwords</th>
</tr>
</thead>
<tbody>
<tr>
<td>simarsingh</td>
<td>tackcalb</td>
</tr>
<tr>
<td>rusty</td>
<td>rdhrs!#</td>
</tr>
<tr>
<td>123456</td>
<td>109$jocularity3#34</td>
</tr>
<tr>
<td>qwerty</td>
<td>Le2MsTe#WdGoRd</td>
</tr>
<tr>
<td>basketball</td>
<td>ec$aatke</td>
</tr>
<tr>
<td>okcthunder</td>
<td>te4grat^</td>
</tr>
<tr>
<td>password</td>
<td>tk#me$tote&amp;mo</td>
</tr>
</tbody>
</table>

“Good passwords have nothing to do with you, your children or your pets” - Dr Phil Polstra, Professor of Mathematical and Digital Sciences, Bloomsburg University of PA
Email Security

- Keep recovery information
- Monitor recent activity (different devices logged on)
- Keep a strong password
- Two Step verification
- Never open Spam emails
Safe Online Shopping/Browsing

- http vs. https
- Shop on safe networks (Secured networks)
  - Avoid open network (Coffee shop, Traveling)
- Use private browsing mode
- Verify different transactions
- When in doubt - Avoid
- Use safer payment options - Credit cards
- Be vary of personal information asked for - SSN, DOB
- Change your password periodically
Fake Website

Welcome to eBay - Sign in

Sign in to your account

To complete your purchase please sign in to your account.

User ID: 
Password: 

I forgot my user ID or password

Keep me signed in.
(Clear the check box if you're on a shared computer.)

Not an eBay member?
Register now or make your purchase as

Register Guest checkout

No Encryption (Http) on Payment page

OrderID: W00532-146-149653403 Amount: USD 189 Thanks for your shopping on www.bottomheels.com

Credit Card Information

Card Type: 
Credit Card No: 
Expiry Date: 1 / 2015 
CVC/CVV2: 

Billing Address
Safe Website

https://
Safe Online Shopping/Browser

- http vs. https (screenshots of different websites)
- Shop on safe networks (Secured networks)
  - Avoid open network (Coffee shop/Traveling)
- Use private browsing mode
- Verify different transactions
- When in doubt - Avoid
- Use safe payment options - Credit cards
- Be vary of personal information asked for - SSN, DOB
- Change your password periodically
Social Media (Facebook, Twitter)

• Be careful of what you post

• Two factor authentication

• Only accept friend requests from people you know

• Don’t click on advertisement links (Spams, phishing)
Scams on Facebook

**South West Air**

Added 3 new photos.

Awesome News vacation lovers! We are giving away 775 first class flights for you and 5 friends to a dream destination of your choice anywhere in the world and $5,000 spending money!

Rules for entry:
1. Share this photo and comment "Thank You" below.
2. Like Our Page...

**Costco**

Get Costco Gift Card for FREE! (limited time only)
costcocards.info
Costco is currently giving away $1000.00 gift cards to all Facebook users!!

**FunDisney Trips**

November 1 at 11:57 pm · Edited

To celebrate the upcoming holiday season, we're giving away tickets to Disneyland or Walt Disney World to a certain few lucky members!!! To surprise your family and get your tickets, follow the steps below:

Step 1: Click "JOIN" if you're not already a member of the group.
Step 2: LIKE and SHARE this post
Step 3: http://bit.ly/1GWSiWc <= Visit this website and follow the instructions for your chance to win Disneyland tickets!!

We will announce winners each week until November 29, 2015!
CLICK HERE NOW! => http://bit.ly/1GWSiWc

**US Powerball**

Survey Scam

We at ~Powerball~ are currently having a great year and would like to share our good fortune with our loving fans! We are giving free $1 Million Jackpot.

To enter this Contest: You Must Like & Share This Photo, Comment 'Done' and Click the following link --&gt; http://

We will determine the winner on November 25 at 10pm
The winner will be messaged via inbox message.

Good Luck, ~Powerball~

**Survey Scam**

Power Ball

$1 Million

Your Name

Date:

Pay to the Order of:

YOUR NAME

Tom Romero

20,049 shares

View previous comments
www.hoax-slayer.net
Facebook, Google are tracking YOU!

- Turn off cookies
- Turn off targeted Facebook ads
- User private browsing mode
- Limit site linking
Phishing and email scams

- Check the sender’s email
- Do not give out personal information over email
- Do not click on unknown link
- If it’s too good to be true - it probably is!
- Check with bank or the company
Phishing and email scams

- Check the sender’s email
- Do not give out personal information over email
- Do not click on unknown link
- If it’s too good to be true - it probably is!
- Check with bank or the company
How to identify phishing emails

Hello!
As part of our security measures, we regularly screen activity in the Facebook system. We recently contacted you after noticing an issue on your account.

Our system detected unusual Copyrights activity linked to your Facebook account, please follow the link below to fill the Copyright Law form:

http://www.facebook.com/application_form

Note: If you don't fill the application your account will be permanently blocked.

Regards,

Facebook Copyrights Department

From: "Bank of America" customerservice@bankofamerica.com
To: "Jane Smith" jane.smith12@gmail.com
Date: Wed, May 26, 2010
Subject: Fraud Alert – Action Required

Dear Customer,

At Bank of America, your satisfaction is our number one priority. We have recently added an Advanced Online Security option for our customers with online accounts. It is urgent that you go to our website and add Advanced Online Security to your account. Click on the following and update your information www.bankofamerica.com:

If you do not take these steps, in order to protect you, we will put a hold on your account, and you will be required to visit your local branch to verify your identity.

Thank you for helping us to make Bank of America the safest bank on the internet.

If you are receiving this message and you are not enrolled in online banking, sign up now. New online members will automatically be enrolled in the Advanced Online Security program.

Sincerely,

Bank of America Online Security Department
Phishing and email scams

- Check the sender’s email
- Do not give out personal information over email
- Do not click on unknown link
- If it’s too good to be true - it probably is!
- Check with bank or the company
How to identify scams

1. Amazon scam
2. Walmart scam
3. Scam identification
4. Online shopping fraud
5. Retailer email phishing
Phishing and email scams

- Check the sender’s email
- Do not give out personal information over email
- Do not click on unknown link
- If it’s too good to be true - it probably is!
- Check with bank or the company
Best Practices

- Keep machines/devices updated
- Protect your devices
- Guard your personal information (Strong passwords)
- Use secured network (avoid public networks)
- Use private browsing mode
- Avoid clicking advertisements - Spams and Viruses
- Logout of accounts - email, banking, Facebook
- Never plug an unknown usb
Thank You

simar.cybersecure@gmail.com

Cyber-yoda.com