STOPPING CYBERCRIME

A presentation by the

Financial Cybercrime Task Force of Kentucky

KY Dept. of Financial Institutions

DISCLAIMER

- The views expressed in this presentation are solely the presenter's and are not binding upon any state agency. This presentation does not necessarily reflect the views of the Department of Financial Institutions or any official within the Executive Branch.

TASK FORCE ROLE

- The Financial Cybercrime Task Force of Kentucky:
  - DFI internal work group
  - Offers guidance and warnings for the Kentucky financial services industry
- Goal: Identify and address emerging threats in cybercrime and security and protect the integrity of the Kentucky financial system

HARDWARE AND SOFTWARE

- Virus/malware protection
- Update software and install patches
  - *All* software – not just virus protection
- Password protect home networks
  - Never auto-fill or "remember" passwords

CLICKING, SHARING, SAVING …

- Never give out personal information over telephone, fax, email, social media
- Beware of emails and attachments
  - If unsolicited, don't open it
  - If from a friend, still be cautious
- Back up your files
- Be wary online

EMAILS AND MASQUERADES

- **Phishing** - the attempt to obtain sensitive information (password, account info, etc.)
  by pretending to be a trustworthy entity
- **Spoofing** - someone masquerading as another using false data (forged email sender address, false Caller ID display, etc.)
- **Spear Phishing –** (phishing + spoofing) email that appears to be from an individual or business that you know and attempts to get your personal information

EMAILS AND MASQUERADES

- Check before clicking … If still unsure, ask before acting

From: Smith, Bob [mailto:bsmith@knowandtrust.com]
Sent: Tuesday, October 18, 2016 10:18 AM
Subject: You have a new encrypted message from "Bob Smith" <bsmith@knowandtrust.com>

This message was sent securely via an encrypted connection using SecureServer.

You have a Secure Mail message from bsmith@knowandtrust.com waiting to be read.
The message http://badthingshappen.com/
Ctrl+Click to follow link
Access Secure Email

Note: You've received an encrypted message from bsmith@knowandtrust.com
To view your message
Save and open the attachment (message.html), and follow the instructions.
Sign in using your email information: d

This message was secured by **SecureServer** encrypt.

Thanks!
Bob Smith
President
The Company You Know and Trust

EMAILS AND MASQUERADES

- Check before clicking … If still unsure, ask before acting

From: Smith, Bob [mailto:bsmith@knowandtrust.com]
Sent: Tuesday, October 18, 2016 10:18 AM
Subject: You have a new encrypted message from "Bob Smith" <bsmith@knowandtrust.com>

This message was sent securely via an encrypte

mailto:trouble@badactor.com
Ctrl+Click to follow link

You have a Secure Mail message from bsmith@knowandtrust.com waiting to be read.
The message will expire in 30 days.

Access Secure Email

Note: You've received an encrypted message from bsmith@knowandtrust.com
To view your message
Save and open the attachment (message.html), and follow the instructions.
Sign in using your email information: d

This message was secured by **SecureServer** encrypt.

Thanks!
Bob Smith
President
The Company You Know and Trust

PASSWORDS

- Require a password
- Make it unique
  - Don't use manufacturer default or temporary passwords
  - Don't use the same password for all accounts
- Keep it confidential
- Change passwords
  - Every so often just for security
  - Immediately if breach/disclosure
- Choose 2-factor authentication

POOR PASSWORDS AND PINS

- Passwords should NOT:
  - Repeat letters or numbers or use sequences or patterns
  - Use whole words or common phrases
  - Name a specific person, place, thing, date, etc.
- PINs should NOT:
  - Be a number easily identifiable with the user

THE WORST PASSWORDS

Rank	Password		Rank	Password
1	123456		14	abc123
2	password		15	111111
3	12345		16	mustang
4	12345678		17	access
5	qwerty		18	shadow
6	123456789		19	master
7	1234		20	michael
8	baseball		21	superman
9	dragon		22	696969
10	football		23	123123
11	1234567		24	batman
12	monkey		25	trustno1
13	letmein			

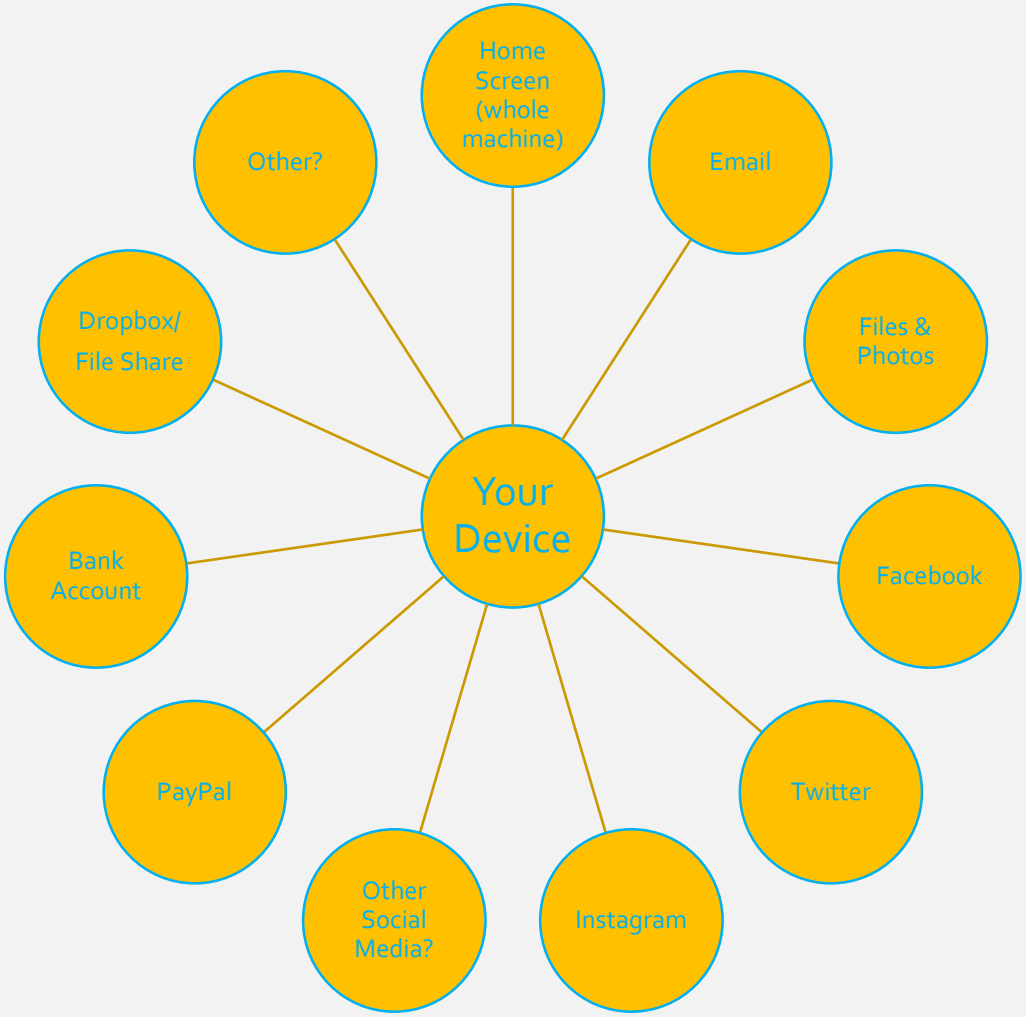
STRONG PASSWORDS

- DO Create Passwords that:
  - Are 8 or more characters
  - Contain uppercase and lowercase letters
  - Contain a number
  - Contain a special character
  - Are unpredictable

Example of a Strong Password:
Prot3ctYfc!
= Protect Yourself From Cybercrime!

CREATE-A-PASSWORD

THINGS PASSWORDS PROTECT



BANKING AND SHOPPING

- Only give info over encrypted websites
  - Your bank will never ask for your personal information by email or phone
  - Look for “https” in the web address
  - Use a designated card for online shopping
- Review transactions regularly for unusual activity
- Check out businesses before buying

SKIMMERS

- Avoid false readers:
  - Pull/gently tug on card reader
  - Check the keypad for a false overlay
  - Check for scratches, tape or glue around the card slot
  - Card reader should not scrape the card
- Avoid cameras:
  - Cover the keypad with a hand while typing in the PIN

SKIMMERS

- Be cautious:
  - Use gas pumps closer to the store or pay inside/choose ATMs that are less remote
  - If you suspect tampering, avoid that reader and notify the business and local law enforcement immediately
- Double check:
  - Review your statements closely and often for any unusual activity
  - Report it immediately if it occurs (bank or card company as well as local law enforcement)
  - Review your free credit report: www.annualcreditreport.com

CELL PHONE PROTECTIONS

- A smartphone is a computer too! Protect it like one.
  - Auto lock and password protect
  - Install updates
- Know your Wi-Fi
  - Turn off Bluetooth when not using it
  - Be wary of public Wi-Fi connections
- Understanding apps
  - They collect (and sometimes share) information
  - Update when available
  - Some apps come with malware

OTHER TIPS

- Avoid GPS and cell phone labels/identifiers
- You probably don't need RFID protectors

- You might want to think about key fobs

QUESTIONS OR REPORTS

- Report cybercrime to the Internet Crime Complaint Center (IC3) at http://www.ic3.gov/default.aspx.
- For more information on this topic, visit these sites:
  - http://www.onguardonline.gov/topics/secure-your-computer
  - https://www.dhs.gov/stopthinkconnect
  - http://kfi.ky.gov/industry/Pages/cybercrime.aspx