REFERENCES

Internet Safety

http://www.aarp.org/money/scams-fraud/info-08-2011/internet-security.html

Identify Theft

Federal Trade Commission (FTC)

File Complaint: https://www.ftccomplaintassistant.gov/

ID Theft Hotline: 1-877-438-4338

Credit Bureaus:

Eqiuifax: 1-888-766-0008

Experian: 1-888-397-3742

TransUnion: 1-800-680-7289

Medical Fraud:

Hotline: 1-800-403-0864

Social Security:

Hotline: 1-800-269-0271

http://oig.ssa.gov/report-fraud-waste-or-abuse/fraud-waste-and-abuse

http://www.ftc.gov/bcp/edu/microsites/idtheft/

Booklet Sponsored by:

Indiana Extension Homemakers Association

Education Focus Group

2015-2016

www.ieha.families.com

For more information contact your County Extension Office

How to Stay Safe in Today's World

- Internet Terminology
- Internet Safety
- Identify/Medical Theft
- Card Skimming
- Remote Controls

INTERNET TERMINOLOGY

APPS (applications): a shortcut to information categorized by an icon
Attachment: a file attached to an e-mail message.
Blog: diary or personal journal posted on a web site, updated frequently.
Browser: a program with a graphical user interface for displaying HTML files, used to navigate the World Wide Web (a web browser)
Click: pressing and releasing a button on a mouse to select or activate the area on the screen where the cursor s pointing to.
Cloud: a loosely defined term for any system providing access via processing powers.
Cookies: a small piece of code that is downloaded to computers to keep track of user's activities.
Cyberstalking: a crime in which the attacker harasses a victim using electronic communication, such as e-mail, instant messaging or post-ed messages.
Document: a written or printed paper furnishing information or evidence.
Download: transferring of information from a remote computer to your computer, mobile device or game console.
Hacker: the act of a person who secretly accesses a computer system in order to obtain information or cause damage.
HTML: Hyper-text Markup Language—the computer language that a website uses to display graphics and words on the WWW.
Http: hyper-text transfer protocol— foundation of data communicaton.
Https: hyper-text transfer protocol with security—includes banking, investment, e-commerce and most websites that require a log-in.
Icon: a representative symbol of an app.
Link: a highlighted or underlined feature on a web page that, when clicked will take you to another web page.
Malware: a program designed to damage a computer, collect information or remotely take over the computer.
Mouse: input device used with a personal computer. Involves moving or clicking a button.

NOTES

Car Key Remote Entry & Car Starters — The key fobs that are available to open our cars send off a radio signal. Thieves have found a way to extend that radio signal that goes between your key fob and your car. Even if your fob was inside your house, an extender or amplifier would make your car think it was close by. The doors would unlock. Here are a few safety precautions:

1. Keep your keys in a metal box when you are home. This stops the signal from being extended.

2. Carry your keys in a wallet or purse designed to thwart hacks of passports or credit cards with radio-frequency ID chips (RIFD).

3. Some people put their keys in the refrigerator or freezer. This is not recommended as lithium batteries need to be stored above 68 degrees Fahrenheit to be effective.

4. Parking your car in a locked garage or in a well-lit place could deter technologically savvy thieves.

Passwords: an arbitrary string of characters chosen by a user in order to prevent unauthorized access to an account.
Pharming: the fraudulent practice of directing Internet usage to a bogus website that mimics the appearance of a legitimate one in order to obtain personal information, such as passwords, account numbers, etc.
Phishing: the act of requesting information needed to steal a victim's money or identification.
Pop-up: a window that suddenly appears when selecting an option with a mouse or pressing a special function key. Can be blocked in settings.
Posting: uploading information to the web.
Search engine: an Internet service that allows you to search for information and documents on the web.
Social media: forms of electronic communication that are used by large groups of people to share information and develop social and professional contacts, such as Facebook, Flicker, Instagram, Twitter, etc.
Spam: known as junk e-mail.
Spellcheck: flags words in a document that may not be spelled correctly and also checks grammar and punctuation.
Streaming: the activity or listening to or watching sound or video directly from the Internet.
Unsubscribe: cancel a subscription to an electronic mailing list online service.
Upload: transfer information from your computer to a website on the Internet.
Username: Also called login name, logon name, sign-in name, sign-name. a unique sequence of characters used to identify a user and allows access to a computer system.
Virus and Spyware: Harmful programs that spread by sending copies of itself to other devices hidden in code or attached to documents.
Webpage: electronic, digital document created with HTML and accessible with a browser.
Website: a collection of documents called web pages.

Internet Safety Tips

People hear stories about the risks of being on the Internet and all of the bad things that can happen. This scares them and they do not want any part of the Internet. This is a real shame because the Internet is a wonderful place to learn, communicate, shop, bank, get help and be entertained. By learning just a few safety precautions, you can be just as safe on the Internet as you are in your everyday life.

1. Understanding the Internet -- Online risks occur because of lack of knowledge, carelessness, unintentional exposure to personal information, technology flaws, lack of consumer protection and criminal acts. With a little knowledge, most of these risks can be minimized and keep you safer.

2. Safe Technology -- No matter how safe you are online, if your computer becomes infected with viruses or spyware, your information could be stolen and your safety compromised. Here are a few things you can do to avoid this:
   a. Protect your computer by installing antivirus and anti-spyware software. Set these to automatically update. There are good, free antivirus services such as AVG and McAfee. There are also free anti-spyware services like Ad-Aware and Spybot.
   b. Use a reputable browser such as Google Chrome, Microsoft Edge or Firefox. Keep the default security and privacy settings intact.
   c. Keep up to date. Set your system so that it automatically checks for and installs software updates for your Operating System and Browser.
   d. Turn on your firewall, which is a part of your computer system or network, that blocks unauthorized access while permitting outward communication. The firewall is managed through the Control Panel.
   e. If you're using a home wireless network, make sure security is enabled for it. Check your settings.

Ask a computer-knowledgeable friend, son, daughter or grandchild to help you if this sounds complicated.

REMOTE CONTROLS

Garage Door Remote Control Safety—Some thieves are able to "record" your transmitter's signal. Later, after you're gone, they replay that signal and open your door. Here are a few precautions you can take.

1. If your transmitter (the remote control) has rolling code technology, the code changes after every use. This renders the thieves' controls useless. Contact your garage door opener manufacturer or your local garage door dealer for more information.

2. While on vacation, unplug the garage door opener unit or use a wall vacation lock console security switch. This is an optional accessory to most openers. It will insure no one is able to open your garage door while you and your family away.

3. Change the manufacturer's standard access codes on the opener and remote control. Newer models of openers have rolling-code technology, which changes the access codes each time the opener is used to prevent code grabbing. Be sure to change the manufacturer's standard access codes on the opener and remote control. Consider investing in a newer model with more safety and security features that are now standard.

4. Never leave the remote control in the car or with a parking attendant. A new trend in home invasion is gaining access to the home by stealing the opener or car. Consider using a key chain remote and always lock the entry to the inside of your home – especially if your opener is programmed to your vehicle. It is a small inconvenience for safety and security.

2. Wiggle everything. ATM's are solidly constructed and don't have any loose parts. The keyboard should be securely attached. When you insert your card, give it a wiggle. This won't interfere with your transaction but will foil the skimmer.
3. Cover your hand when you enter your PIN number. Skimmers must have the PIN number or else they can't use the card.
4. Skimmers are installed on ATMs that aren't located in busy locations such as on the sidewalk. ATM's in banks and groceries are much safer.
5. The chances of getting hit by a skimmer are higher on the weekend than during the week, since it's harder for customers to report the suspicious ATMs to the bank. Criminals typically install skimmers on Saturdays or Sundays, and then remove them before the banks reopen on Monday.

If you don't notice a card skimmer and your card data does get stolen, not all is lost. As long as you report the theft to your card issuer (for credit cards) or bank (where you have your account) as soon as possible, you will not be held liable for the lost amount and your money will be returned. Business customers, on the other hand, don't have the same legal protection and may have a harder time getting the money back.

Just remember: If something doesn't feel right about an ATM or gas pump, don't use it.

3. Browsers, Search Engines & Anti-virus Software —Browsers help you move around the Internet. Search engines make it easy to find information on the Internet. A secure browser along with an anti-virus/anti-spyware program helps you identify safe and unsafe websites. A secure browser would be Chrome, Firefox or Microsoft Edge. Safe search engines are Google, Bing and Yahoo just to name a few.
    a. If you get a notification from your antivirus/malware program that a site you are trying to visit is unsafe, do not open web page.
    b. If a site asks you to change your browser settings in order to get better and faster service, ignore the request and visit a different website.
    c. Allow downloads and execution of programs only when you're absolutely sure you understand what the program will do.

    Again, ask a computer-knowledgeable friend, son, daughter or grandchild to help you if this sounds complicated.

4. E-Mail Safety -- Adopt the following e-mail practices for safer computer usage every time you send or receive messages.
    a. Don't share sensitive personal information and never share passwords, social security numbers and credit card numbers in an e-mail.
    b. Be particular who you e-mail. If someone sends you an e-mail, it doesn't mean you need to read or respond to the e-mail. Set your spam filters to be restrictive and check your spam folder periodically for legitimate messages.
    c. Be careful before opening attachments or clicking links in an e-mail. If you don't know the sender, delete the e-mail. If you do know the sender but weren't expecting an attachment, double-check that the person actually sent the e-mail.

d. When sending e-mail to a group of people who don't know each other, use the bcc (blind carbon copy) line to protect everybody's Identity. By doing this, no recipient can see the e-mail addresses of the other recipients. This respects their privacy and protects their accounts from spammers.

5. Passwords – Strong passwords don't have to be hard to remember, just hard to guess. Strong passwords use at least 10 characters and include uppercase letters, special characters (such as #, @) and numbers. Avoid personal identification such as birthdates, addresses, etc. To make it easy, use a phrase, song or a rhyme. For example:

   a. 2BorNot2B (to be or not to be)
   b. John3:16-17 (Biblical verse)
   c. 3blindMice (three blind mice)
   d. thimStreboR (Robert Smith backwards)

6. Fraud and Scams – Most e-mail spam and scams are easy to spot. Here are some red flags.
   a. You don't know the person sending the e-mail.
   b. The claims sound too good to be true.
   c. Someone is promising to send you money or a prize.
   d. A store, bank, environmental agency asks for your account information and password.
   e. You're asked to click on a line and download a file.
   f. The message has misspellings and sounds unprofessional.

7. Sharing Photos – Posting pictures online is a good way to share experiences with others. Only share with those who know you well. Be cautious if you want to share photos publicly.
   a. Understand what information is in a photo. Consider not what you think you are sharing but what a criminal or bully can glean from the photo.

CARD SKIMMING SCAMS

Skimming—This is like identity theft for debit cards: Thieves use hidden electronics to steal the personal information stored on your card and record your PIN number to access the cash in your account. Skimming occurs most frequently at retail outlets that process credit card payments -- particularly bars, restaurants and gas stations.

How skimming works—Skimmers are small devices that can scan and store credit card data from the magnetic stripe. Crooks can install skimmers on a gas pump, ATM machine or other electronic dispensing machine. Corrupt employees can have a skimmer stashed out of sight of customers. Once the card is run through the skimmer, the data is recorded, Crooks can sell the information through personal contact with others or on the Internet. Counterfeit credit cards are then produced for them to use or to sell to other thieves. The criminals go on a shopping spree with a cloned copy of the credit or debit card, and cardholders are unaware of the fraud until a statement arrives with purchases they did not make.

Here are some tips to check when you're at the ATM:

1. Check for tampering—at the top of the ATM, near the speakers, the side of the screen, the card reader and the keyboard. If something looks different (a different color, graphics are misaligned or anything else that doesn't look right, don't use the ATM). If the keyboard doesn't feel right (too thick maybe), there could be a PIN-snatching overlay, so don't use it.

SYNTHETIC IDENTITY THEFT

This is a new version of identity theft. Information is stolen from several people to create a new identity using someone's name and combining it with someone else's social security number and someone else's address thereby creating a new account. This type of theft is hard to identify because it isn't directly tied to one person. Children's social security numbers are often target in these frauds.

Again, check your credit report for accounts you did not open and ask the credit report agency if there is a fragmented file (sub-account using your SSN but not your name) attached to your main credit file. Report all cases of Synthetic Identity Theft to the Federal Trade Commission.,

TAX-RELATED IDENTITY THEFT

This occurs when someone uses your stolen Social Security Number to get a tax refund or a job. Warning signs are:

A. If more than one tax return was filed using your SSN.
B. You owe additional tax, you have had a tax refund offset, or you have had collection actions taken against you for a year you did not file a tax return.
C. IRS records indicate you received wages from an employer unknown to you.

The IRS doe not initiate contact with a taxpayer by sending an e-mail, text or social message requesting personal or financial information. If you get one of these messages, do not reply or click on any links. Instead, you should report it to the IRS.

b. Some types of photos can be used in unintended ways such as to embarrass you or threaten you .

8. Spreading and Collecting Information – Sharing personal information with friends and family enriches relationships. Sharing personal information with untrustworthy people is taking a risk. Be careful when sharing the following pieces of information:
    a. Addresses and phone numbers.
    b. Names of family members (including mother's maiden name)
    c. Information about your personal property, work history or financial status.

9. Emotional Exposure – Offline criminals read birth, wedding and obituary announcements in the newspapers to find possible victims. Online criminals do the same thing. Follow these guidelines for safely sharing joy or grief in any public online setting.
    a. Choose whether you want the site private (only those whom you allow) or public (available to anyone). Then decide the Information to provide.
    b. Let others know your safety boundaries so they can participate online in a way that respects your privacy choices.
    c. If you're too busy, ask a friend to monitor the site for Information risks so you can focus on other matters.
    d. If you choose to place contact information online, create a separate e-mail address for this purpose to protect your main e-mail address.

10. Report Abuse – Often people don't know where to turn when something has gone wrong online. Every site should have an easy-to-find "Report Abuse" feature and a way to contact customer support. Additionally, if your safety is threatened, or a crime has been committed, contact your local law enforcement office. It will bring in other agencies, attorney general, etc. if needed. Immediately report dentity theft to your local law enforcement agency, as well as to credit reporting agencies.

IDENTIFY THEFT

Identity (ID) theft is when a thief steals your personal information, such as your full name or social security number. Theives can use this information to apply for credit, file taxes, or get medical services. This can damage your credit and cost you time and money. You may not know that you are a victim of ID theft until you experience mystery bills, credit collections or denied loans. Several common types of identify theft are:

1. Child ID Theft—Children's ID's are vulnerable because the theft may go undetected until they are adults. This undetected fraud will be harder to correct because of the time that has passed.
2. Tax ID Theft—Your social security number is used to falsely file tax returns with the IRS or State government and to receive tax refunds.
3. Medical ID Theft—Your Medicare ID or health insurance member number is used to get medical services or to issue fraudulent billing to your health insurance provider.
4. Senior ID Theft—Seniors are citizens are more vulnerable due to more frequent contact to medical services because of age and health issues. Seniors are a more trusting population and are more easily scammed.
5. Social ID Theft—Your name, photos and other personal information is used to create a phony account on social media.

HOW TO PREVENT IDENTITY THEFT

1. Secure your social security number. Don't carry your S.S. card in your wallet or write your number on your checks. Only give out your SSN when absolutely necessary.
2. Don't respond to unsolicited requests for personal information (name, birthdate, SSN, or bank account number) by phone, mail or Internet.
3. Watch out for "shoulder surfers." Shield the keypad when typing your passwords on computers and at ATMs.
4. Collect mail promptly. Ask the post office to put your mail on hold when you are away from home.
5. Pay attention to your billing cycles. If bills or financial statements are late, contact the sender.

6. Review your receipts. Compare receipts with account statements. Watch for unauthorized transactions.
7. Shred receipts, credit offers, account statements and expired credit cards. This prevents "dumpster divers" from getting your personal iinformation.
8. Store personal information in a safe place at home and work.
9. Install firewalls and virus-detection software on your computer.
10. Create complex passwords. Change passwords occasionally.
11. Order your credit report once a year and review it to be certain it doesn't include accounts that you have not opened.

REPORT IDENTITY THEFT

If you are a victim to identity theft, report it immediately to the Federal Trade Commission.

1. The FTC will give you an ID theft affidavit.
2. Print this affidavit and take with you to your local police to file the crime and get a police report.
3. These two documents are your identity theft report. These reports are important to help you resolve problems with creditors, banks and other companies.
4. Report specific types of identity theft to other agencies such as:
    - A. Long-term Care (report claim to the long-term care ombudsman in your state if theft was result of a stay in a nursing home or long-term care facility).
    - B. Medical (your health insurance's fraud department or Medicare's fraud office)
    - C. Tax (report this to the IRS and your State's Department of Taxation or Revenue)
    - D. There are three credit report agencies that can freeze your accounts so that no one can apply for credit in your name.
    - E. Financial Institutions (banks, credit card companies and other places you may have accounts)
    - F. Retailers and Other Companies
    - G. State Consumer Protection Offices or the Attorney General.