Think Before You Click (Ages 13-17)

Introduction

Hey teens! The internet is an incredible tool for connecting with friends, exploring new interests, and learning. But just like in the real world, there are risks online that you need to be aware of. This guide, “Think Before You Click,” is all about helping you become a savvy digital citizen. We’ll explore common online threats like phishing and scams, and give you practical tips to protect yourself, your information, and your devices. Learning to pause and think before you click is one of the most powerful ways to stay safe online.

Understanding Online Threats: Phishing, Scams, and Social Engineering

Cybercriminals are always looking for ways to trick people online. They often use clever tactics to get you to reveal personal information or click on harmful links. Understanding these threats is the first step to protecting yourself [2].

1. Social Engineering: The Art of Manipulation

Social engineering is a tactic cybercriminals use to manipulate people by playing on emotions like trust, fear, or urgency. Their goal is to get you to act quickly without thinking, often by pretending to be someone you know or trust, like a bank, a company, or even a friend. They use deception and impersonation to make their messages seem real [2].

2. Phishing: The Most Common Bait

Phishing is a type of social engineering where someone sends a fake message that appears official, hoping you’ll click a link or give away sensitive information. These messages can come via email, text (smishing), or even fake websites. The links often

look legitimate but are designed to steal your passwords, credit card numbers, or login details [2].

Types of Phishing:

- **Deception Phishing (Impersonation-based)**: The attacker pretends to be a legitimate organization (e.g., your bank, school IT department, or a popular online store). They might also impersonate individuals in positions of power, like a teacher or principal. The email or communication might even come from a legitimate account that has been compromised [2].
    - **Example**: You receive an email that looks exactly like it's from your school's IT department, saying your account will be locked if you don't click a link to verify your password. The link leads to a fake login page.

- **Spear Phishing & Whaling**: These are more targeted attacks. Spear phishing targets specific individuals, while whaling targets high-profile individuals (like a school administrator). Attackers often research their targets to make the messages highly personalized and convincing [2].
    - **Example**: You get a text message that seems to be from your coach, asking you to click a link to view an updated game schedule, but the link is malicious.

- **Clone Phishing**: This involves creating an exact replica of a legitimate, previously delivered email, but replacing its links or attachments with malicious ones. The attacker then sends it from a spoofed email address [2].
- **Phishing Without Impersonation**: These attacks don't necessarily pretend to be a specific entity but use generic urgent messages to trick you into clicking. They might offer free games, gift cards, or warn of a security breach [1].

3. Other Scams to Watch Out For:

- **"Too Good to Be True" Offers**: Free games, gift cards, or exclusive content that seems too good to be true often come with hidden costs, like giving away your personal data or downloading malware [1].
- **Pop-Up Ads**: Be wary of pop-up ads that claim your computer has a virus or that you've won a prize. These are often designed to trick you into downloading harmful software or giving up information [1].

- **Romance Scams**: While more common for adults, some predators build emotional connections online to manipulate and exploit teens [3].

Your Digital Toolkit: How to Protect Yourself

Staying safe online isn't about avoiding the internet; it's about using it smartly. Here are some essential habits and tools to protect yourself from online threats [1, 3].

1. Be Skeptical and Verify:

- **Pause Before You Post/Click**: Always take a moment to think before you click on a link, download a file, or share personal information. If something feels off, trust your gut [1].
- **Check the Sender**: Look closely at the sender's email address or username. Is it exactly what you expect? Cybercriminals often use slight misspellings or unusual domains (e.g., `.net` instead of `.com`) [1].
- **Hover Over Links (Don't Click!)**: Before clicking a link, hover your mouse over it (on a computer) or long-press it (on a phone) to see the actual URL. If it doesn't match the expected website, don't click [2].
- **Verify Urgent Requests**: If you receive an urgent request for information (especially passwords or money) from someone you know, contact them through a different, verified channel (like a phone call or a new email) to confirm it's legitimate. Don't reply directly to the suspicious message [2].
- **Is it Legitimate?**: Malicious websites can look identical to trusted sites. Always check the URL in the address bar. If in doubt, avoid the website [1].

2. Protect Your Accounts and Devices:

- **Strong, Unique Passwords**: Use a combination of uppercase and lowercase letters, numbers, and symbols. Never reuse passwords across different accounts. Consider using a password manager to keep track of them [1].
- **Two-Factor Authentication (2FA)**: Enable 2FA on all your important accounts (email, social media, gaming). This adds an extra layer of security by requiring a second verification step, like a code sent to your phone [3].

- **Keep Software Updated**: Regularly update your operating system, web browsers, and apps. Updates often include important security fixes that protect you from new threats [1].
- **Antivirus Software**: Ensure your computer has up-to-date antivirus software installed and running. This helps detect and remove malicious programs [1].
- **Be Careful with Free Wi-Fi**: Public Wi-Fi hotspots are often not secure. Avoid accessing sensitive accounts (like banking or email) when using public Wi-Fi, as your data could be intercepted [1].

3. Manage Your Digital Footprint:

- **Privacy Settings**: Regularly review and adjust the privacy settings on all your social media accounts and apps. Control who can see your posts, photos, and personal information [3].
- **Think About What You Share**: Information about you, like your interests, location, or photos, has value. Be selective with what you provide online. Remember, anything you post can be easily copied and can live on the internet forever, even if you delete it [3].
- **Don’t Share Sensitive Information**: Never share your full name, address, phone number, birthdate, Social Security number, or financial information with anyone online unless absolutely necessary and verified by a trusted adult [3].

What to Do If You Clicked or Shared Something Suspicious

Even the savviest internet users can make mistakes. If you suspect you’ve fallen for a scam or clicked on a malicious link, here’s what to do:

1. **Disconnect Immediately**: If you clicked a suspicious link or downloaded something, disconnect your device from the internet (turn off Wi-Fi or unplug the Ethernet cable) to prevent further damage.
2. **Change Passwords**: Immediately change the passwords for any accounts that might have been compromised, starting with your email and banking accounts. Use strong, unique passwords.

3. **Run a Scan**: Run a full scan with your antivirus software to check for and remove any malware.
4. **Inform a Trusted Adult**: Tell a parent, guardian, teacher, or school IT staff member what happened. They can help you assess the situation and take further steps.
5. **Report the Incident**: Report phishing emails to your email provider. If you shared financial information, contact your bank. If you believe you've been a victim of a cybercrime, you can report it to relevant authorities.

Conclusion

Being online is a huge part of being a teenager today, and with great power comes great responsibility! By adopting a "Think Before You Click" mindset, understanding common threats, and using the tools available to you, you can navigate the digital world safely and confidently. Remember, your online safety is in your hands, and trusted adults are always there to help you if you need it. Stay smart, stay safe, and enjoy the internet responsibly!

References

[1] Internet Safety for Kids - The Annie E. Casey Foundation. (2025, March 7). *The Annie E. Casey Foundation*. https://www.aecf.org/blog/internet-safety-for-kids [2] Think Before You Click | FIU IT Security Office. (n.d.). *Florida International University*. https://security.fiu.edu/training/think-before-you-click/ [3] Online Safety Tips for Teens | NCDIT. (n.d.). *NCDIT*. https://it.nc.gov/resources/online-safety-privacy/tips-guidance/online-safety-tips-teens