Protect Myself from Cyber Attacks

The National Cybersecurity and Communications Integration Center's (NCCIC) mission is to reduce the risk of systemic cybersecurity and communications challenges in our role as the Nation's flagship cyber defense, incident response, and operational integration center. Since 2009, the NCCIC has served as a national hub for cyber and communications information, technical expertise, and operational integration, and by operating our 24/7 situational awareness, analysis, and incident response center.

Next Steps (#)

- **Never click on links in emails**. If you do think the email is legitimate, whether from a third party retailer or primary retailer, go to the site and log on directly. Whatever notification or service offering was referenced in the email, if valid, will be available via regular log on.
- **Never open the attachments**. Typically, retailers will not send emails with attachments. If there is any doubt, contact the retailer directly and ask whether the email with the attachment was sent from them.
- **Do not give out personal information** over the phone or in an email unless completely sure. Social engineering is a process of deceiving individuals into providing personal information to seemingly trusted agents who turn out to be malicious actors. If contacted over the phone by someone claiming to be a retailer or collection agency, do not give out your personal information. Ask them to provide you their name and a call-back number. Just because they may have some of your information does not mean they are legitimate!

- **Set secure passwords and don't share them with anyone.** Avoid using common words, phrases, or personal information and update regularly.
- **Keep your operating system, browser, anti-virus and other critical software up to date.** Security updates and patches are available for free from major companies.
- **Verify the authenticity of requests from companies or individuals by contacting them directly.** If you are asked to provide personal information via email, you can independently contact the company directly to verify this request.
- **Pay close attention to website URLs**
  Malicious websites sometimes use a variation in common spelling or a different domain (for example, .com instead of .net) to deceive unsuspecting computer users.
- **For e-Mail,** turn off the option to automatically download attachments.
- **Be suspicious of unknown links or requests sent through email or text message.** Do not click on unknown links or answer strange questions sent to your mobile device, regardless of who the sender appears to be.

Learn More

- Advice about common security issues for non-technical computer users (https://www.us-cert.gov/ncas/tips)
- Information about current security issues, vulnerabilities, and exploits (https://www.us-cert.gov/ncas/alerts)
- Weekly Summary of New Vulnerabilities (https://www.us-cert.gov/ncas/bulletins)
- OnGuardOnline.gov (20190822160458/http://onguardonline.gov/)

Stop. Think. Connect. (#)

The Stop.Think.Connect. Campaign (https://www.dhs.gov/stopthinkconnect) is a national public awareness campaign aimed at increasing the understanding of cyber threats and empowering the American public to be safer and more secure online.

Tips (#)

Most people use passwords that are based on personal information and are easy to remember. However, that also makes it easier for an attacker to guess or "crack" them.

For example, instead of the password "hoops," use "IlTpbb" for "[I] [l]ike [T]o [p]lay [b]asket[b]all." Using both lowercase and capital letters adds another layer of obscurity. Your best defense, though, is to use a combination of numbers, special characters, and both lowercase and capital letters. Change the same example we used above to "Il!2pBb." and see how much more complicated it has become just by adding numbers and special characters.

Last Published Date: November 5, 2018