Person giving the Flash talk: Evaluator: _____

Practice PT - Flash Talk: The Internet and Society

Record your research in the organizer provided here:

My Selected issue: DNS vulnerabilities
Focus of my flash talk: Hillary Clinton's unsecured email server
The position I will take in my talk: Politicians should demonstrate that they are well-informed on how technology works and what measures they should take to keep information of national importance secure.

What is the reference? What did I learn from this reference?	**What are the positive (+) and negative (-) impacts on society, economy, or culture? What do I want people to know about this?**	**What are the connections can I make to what I've learned about the Internet so far?**	**What details have I learned that support the position I have taken on this issue?**
Reference 1 (wikipedia) https://en.wikipedia.org/wiki/Hillary_Clinton_email_controversy While in office, Clinton used her family's private server rather than a government one to send and host official emails.	The FBI discovered that over 2,000 of these emails contained confidential information-- 2,000 emails that foreign agencies and hackers may have had access to. This compromised national security, and cast aspersions on Clinton's ability to handle matters of national importance. It also reflected negatively on her presidential campaign.	Unsecured servers can be manipulated by hackers, as has happened in the past before and as hackers tried to do so with Clinton's email server.	Clinton used a private email server in her home basement, rather than a federally secured one. The FBI concluded that this left her emails extremely vulnerable to unfriendly eyes.
Reference 2: http://www.huffingtonpost.com/michael-gregg/six-ways-hillary-clintons_b_8071822.html The "man in the middle" approach was one way hackers might have gained access to her emails.	There are no positive impacts; Clinton's emails could have been accessed in so many ways, including simply brute-force guessing her passwords. Hackers might also have set up a fake server to redirect Clinton's emails. This would have been especially easy because Clinton kept her email server in the basement of her New York home.	DNS poisoning, or man-in-the-middle, means that if a user tried to connect to Clinton's email, they would be redirected to a mirror website, where they would unknowingly feed national information to the hackers.	Clinton's lack of technological savviness meant that she left her emails vulnerable in all sorts of ways like this. That a person with her level of responsibility was so ignorant about Internet security is disturbing.

Person giving the Flash talk: Evaluator: _____

Practice PT - Flash Talk: The Internet and Society

Reference 3: http://www.livescience.com/55349-how-email-servers-work.html This reference explains in detail how email servers work, what information they contain, and how the SMTP and POP3 servers work together to handle incoming and outgoing mail.	The technology behind emails is very complicated, as shown in this article. I want people to understand this complexity so that they can make informed judgments on whether Clinton should have been more careful, and going forward, how educated politicians should be in these matters.	Ever email server, including the one in Clinton's home, has an SMTP server, which handles outgoing email. If an email is being sent to a different domain than its sender's address, the SMTP server will have to ask the DNS for the IP address of the recipient before it can send the email.	An SMTP server managed by a private individual, as Clinton did, leaves outgoing mail susceptible to attacks, highlighting gaping holes in our national security.

Making Email Great Again

Forget about building a wall, letting in refugees, or fixing the economy-- the question we should be asking our politicians is, do they understand how email protocols work? And can they be trusted to keep their emails safe from hackers? Hillary Clinton obviously didn't.

In the last year, it came to light that while in office, Clinton used a private email server in her family home basement rather than a government one for official communications. This meant that national correspondence was left vulnerable to foreign hackers. Clinton has claimed that she was not "technologically sophisticated" enough to understand how emails worked; if that's true, here's what she didn't know.

All email hosts rely on an SMTP server, which handles outgoing email. If you send an email to someone with an address from a different domain, such as from a .gov address to a .org address, the SMTP server has to ask the DNS to look up the other person's IP address before it can send the email.

When the server is hosted by a private individual, as in Clinton's case, it is especially vulnerable to a man-in-the-middle attack. In this attack, when the SMTP server contacts the DNS for the IP address, it will be redirected to a fake website, hosted by foreign hackers, so that the emails fall into the wrong hands. And Clinton claims that she was unaware of all this, and thought that her emails were safe enough on her family server.

I think we can all agree that the American people deserve representatives who understand how technology works and who care about national security. Every politician should be required to answer these questions: do you know where your emails are going? Do you know who might be reading them, other than the NSA? Do you know how to keep them secure? If our government wants to make America great again, their first step should be making emails great again!