4-1-2019

BCoE Creates Internet Safety Checklist

Broadband Center of Excellence (BCoE)

safety checklist

BCoE Creates Internet Safety Checklist

The University of New Hampshire Broadband Center of Excellence (BCoE) has created a checklist for individuals to use in assessing their vulnerability to threats originating from their use of the Internet wherever they are linked — home or public place.

"At a time when hackers create chaos and are able to gain remote control of automated cars or in-home baby monitors, it is incumbent for us all to take responsibility for Internet safety and not passively trust governments, organizations and service providers to do it for us."

BCoE Executive Director Dr. Rouzbeh Yassini

And the effect of broadband continues to grow. At the end of last year it was widely reported that more of us than ever have Internet access with more than 50% of the world's population now online. Add to that the 125 billion Internet of Things (IoT) devices expected by 2030 and the breadth of available targets of vulnerability becomes apparent.

This BCoE document provides a self-assessment of how one configures, maintains and uses Internet-connected devices, computers, applications and networks under their direct control in a grouping called the Digital Home while providing cautionary warnings of areas outside the Digital Home that we like to call the Internet Wilderness.

University of New Hampshire
Broadband Center of Excellence

Identification and protection from Internet threats to the Digital Home are grouped into 3 areas with the following table providing examples that fall into each group. We also provide analogies to our physical homes to help clarify the groupings:

CLASSIFICATION	DIGITAL HOME	PHYSICAL HOME
Security	Firewall and Router	Doors and Windows
Safety	Access Control and password maintenance	Locking doors and windows
Privacy	File encryption and social media configuration	Lowering the blinds

BCoE defines Internet Security, Safety and Privacy as follows:

- **Security:** the physical means (router, firewall) of preventing or reducing risk of harm to the Digital Home from Internet-based threat
- **Safety:** the act (passwords, threat analysis) of protecting the Digital Home from Internet-based threats
- **Privacy:** the preventing of unauthorized usage of personal information and data (safe web sites, secure data storage, application privacy configuration)

These groupings in the Digital Home have analogies to our physical home that we maintain to protect our families, loved ones and personal possessions:

Security is the physical means of controlling access to the home provided by the windows, doors, security lighting and alarm systems, establishing the first level of protection. With these means we might feel secure but we are not yet necessarily safe. Similarly access to the Digital Home is provided by access points that normally include a router and/or firewall.

Safety is securing the physical means of controlling access to the home and detecting illicit intrusion accomplished by locking outside doors and windows, arming alarm systems and turning on security lighting. In the Digital Home this is accomplished by properly configuring the routers and firewalls while making sure the software of all devices touching the Internet is up to date.

Privacy in the physical Home can be provided by lowering the window blinds and curtains to prevent outside observation. Analogies in the Digital Home include securing private files, proper configuration of social networking applications and care in disseminating personal information when accessing web sites. In our physical homes we might also want to invite a neighbor into our home but for privacy reasons restrict them to certain areas by closing appropriate inner doors. In the Digital Home this is analogous to having a separate private and guest Wi-Fi network.

"Creating a digital home environment that is totally invulnerable to Internet threats is very difficult and some might say impossible," Yassini said. "The bad guys are evolving their tactics and becoming more sophisticated, and a new threat evolves for every protection," he added.

The BCoE recommends that individuals evaluate their personal situation as they are able, and implement steps to protect their Internet security, safety and privacy as facilitated by the BCoE self-evaluation survey document. As an example of the challenges, BCoE ran the survey with industry professionals and found that even these sophisticated users were only 75% protected from known threats.

In keeping with the understanding that personal responsibility to protection from Internet threats is key BCoE laid out several premises.

- Internet threats do not just originate from organized crime, hostile foreign governments or hackers locked in their dark bedrooms, but also from our largest corporations and service providers, especially in the area of privacy. Since there is informational and monetary value in data collected on Internet usage an individual should expect that their usage will be monitored and exploited.
- Individuals should understand the distinction between their private network (Digital Home) that should only be accessible to those they authorize and the public Internet (Internet Wilderness) that is accessible to all with no restrictions. Clear points of demarcation should always exist between the two and these points must be well understood and properly configured.

Before an assessment can be made it is important to determine a person's mindset toward usage of the Internet since this can determine the depth of protection taken. Not everyone uses the Internet in the same way or has equal concerns and understandings. There are many thoughts on this and here are a few we have come across:

- Billions of people use the Internet so what is the probability of someone attacking me?
- I don't use the Internet for anything personal or financial, so I don't care if I am attacked.
- I don't understand what I can do so I'll just ignore the problem.
- I can't be bothered, I don't have the time, Its somebody else's problem.
- My service provider or government or web sites have my best interest at heart so why should I worry
- I use a Macintosh and my service provider installed a router on my home network, so I am well protected

Protecting oneself from Internet threats is not an all or nothing effort. Each item addressed on the list reduces one's risks of being the victim of an attack and is worth doing.

The BCoE document covers many areas, but even taking a few basic steps will help significantly:

- Keep software up to date. Do not procrastinate in updating.
- Never trust unsolicited emails, never go to a company's web site using a link in the email, never respond with any personal information and never try to open an attached file. Go directly to the company through their web site, or call.
- Always use passwords that would be difficult to guess, change default passwords on Internet connected devices and use two-level authentication when possible.
- Always verify whom you are communicating with and be leery of unsolicited invitations from anybody, including collaboration applications.

This survey instrument is not all inclusive and BCoE intends in future iterations to explore other threats to our connected world, including with autonomous autos.