8-1-2006

Digital Hygiene: Clean Living on a Dirty Network

Charles Boulet

Follow this and additional works at: http://commons.pacificu.edu/inter06

Recommended Citation


This Article is brought to you for free and open access by the Interface: The Journal of Education, Community and Values at CommonKnowledge. It has been accepted for inclusion in Volume 6 (2006) by an authorized administrator of CommonKnowledge. For more information, please contact CommonKnowledge@pacificu.edu.
Digital Hygiene: Clean Living on a Dirty Network

Rights
Terms of use for work posted in CommonKnowledge.

This article is available at CommonKnowledge: http://commons.pacificu.edu/inter06/17
Digital Hygiene: Clean Living on a Dirty Network

Posted on September 1, 2006 by Editor

By Charles Boulet <cboulet@verizon.net>

Why ‘Digital Hygiene’? Since the creation of ENIAC, the term digital has been synonymous with progress, scientific advancement, and the futuristic evolution of technology. At the same time, hygiene is a term that is reminiscent of long and tedious grade-school lectures on manners, making beds, and how to brush one’s teeth properly. Tedious as they may have been, no one will question the value of politesse in a cooperative environment, a comfortable bed to sleep in, or not having to suffer the pain of a root canal. Clearly, what doesn’t kill you makes you stronger.

In one definition, Hygiene is the science that deals with the promotion and preservation of health. In an active sense, hygiene comprises the establishment of conditions and practices that serve to promote or preserve health. With an ever-expanding number of threats to our digital lives, we need to take a new look at an old grade-school standard. Call it Digital Hygiene.

Any discussion of hygiene requires a definition of health. Let us define Digital Health as

- Technical and behavioral soundness in computing habits and platform;
- Freedom from disease or abnormal functioning;
- A condition of optimal technical and behavioral functioning and synergy.

If you are reading this, you are at least curious about computer and network safety and security, but perhaps you also have a definite concern and are looking for real solutions. In this series of articles, you will find definite solutions, but more importantly you will find lessons and skills required to promote and preserve your own digital health. That is, Digital Hygiene shows us all how to maintain healthy, optimally functioning personal computers, and how to operate safely and securely in an open networking environment. Additionally, in the same way courses in personal hygiene enable us to be more responsible in minimizing risks to other people, Digital Hygiene helps us to minimize risks when sharing data with others and to encourage them to do the
same.

The only way to completely eliminate threats on the Internet is to avoid all interactions with it. Whereas is it possible to simply view 'net content much as one watches television, the Internet is designed for collaboration and to use it as a passive television-like medium seems pointless and timid. However, as soon as you open the gates of interactive communication, you are subject to innumerable threats, some mild and others severe, some obvious others hidden.

For example, the simple act of opening your favorite web page illustrates well one simple yet common and powerful avenue of attack. For each IP (Internet Protocol) address, the unique identifier that enables communication between your computer and others on the Internet, there are over 65,000 ports. As an analogy, the IP number identifies the building (your computer), and the ports identify the individual doors open around the building’s periphery. The ports are assigned in three ranges by the IANA (the Internet Assigned Numbers Authority), some are tagged for definite purposes, while others are open for use as individual users and programmers see fit. Only one port, port 80, is used to communicate for the Hypertext Transfer Protocol, or HTTP, when browsing the web. You are, in general terms, aware of what is occurring on this one port while browsing the web. Meanwhile, the remaining ports remain open and unattended. On most Windows XP or Mac OS X systems, many of the ports will be closed, but many remain open and many of the open ports allow function calls that can fully and completely compromise your computer.

The issue of controlling ports is addressed in a later article. Many related concepts and techniques relating to network security and other critical areas are presented throughout this series. Here is an outline of what will be covered in this series in the coming months:

- **Digital Hygiene: Security Tools** — Even with the varied and expanding list of threats to data security, protecting against the vast majority of online threats remains a relatively simple task — subscribe to and install suitable Internet data security solution on each connected computer on your network. While there are many software tools available to provide Internet data security, the differences between them are significant and the choice of tools can be confusing, even frustrating. Some software solutions are comprehensive, while others require addition of supplemental modules to manage all areas of concern. This article will present some of the key components to include in a complete solution and provide the reader with skills and knowledge required to make a sound choice for their own purposes, and will also make some product recommendations.

- **Digital Hygiene: Email Techniques** — While many of the issues surrounding Internet security can be effectively managed with software solutions, there is no software solution that can effectively protect us from our own follies. Indeed, more often than not in the wired world, the strife we experience is self-imposed. As the aphorism goes, ‘when you point your finger, you have three more pointing back at you’. The ‘Finger Pointing’ series of articles will consider how our own actions lead to data loss and system compromise. This
article, the first in the ‘Finger Pointing’ series, will address how our email habits can open holes in our security shields. Using MS Outlook 2003 as a model, this article will present practical and simple guidelines and tips on using email to enhance personal security and that of one’s contacts.

- **Digital Hygiene: Internet Traps and Trails** — This article, the second in the ‘Finger Pointing’ series will continue the previous discussion on self-inflicted data compromise. In this article, the discussion will focus on identifying and avoiding some common traps we fall into while using email, browsing the web, and using instant messaging. In addition, as we maneuver through and navigate through the various avenues on the Internet, we leave information trails that can compromise our data security. These traps and trails are discussed in this article with a special emphasis on protecting children and other vulnerable groups.

- **Digital Hygiene: Hardware Management** — Computer hardware is manufactured to meet various performance requirements, including minimum MTBF (Mean Time Before Failure). While current manufacturing standards and techniques provide hardware components that last longer and perform better than in the past, all hardware, especially hard drives and high-use disc readers, have a limited life span. Indeed, productivity loss and additional costs due to hardware failure are guaranteed, regardless of what the user does to avoid them. The question then lies in how one might minimize the losses and costs. The third article of the ‘Finger Pointing’ series discusses tools and techniques useful in maintaining sound hardware platform health in order to avoid catastrophic data loss.

- **Digital Hygiene: Network Management** — One of the great joys of modern computing is that is so simple to create a personal network at home or in the workplace. From enabling comprehensive and powerful collaboration techniques to creating wireless entertainment or security systems, computers networked for personal use have extended our productivity and our means of enjoying life’s pleasures further than anyone could have imagined. This fourth article in the ‘Finger Pointing’ series discusses techniques used by network spies to snoop and sniff your network for information you don’t want to share. Simple techniques to secure and test network vulnerabilities will be presented with an emphasis on software solutions to monitor weaknesses and block attacks.

- **Digital Hygiene: Document Management** — Not all data loss comes as a result of malicious activities of third parties. Two of the most common causes of data loss is simple user error and lack of education. If you’ve ever simply erased a document or forgotten the location to where you saved it, you have first-hand experience of document management errors. This fifth and final article in the ‘Finger Pointing’ series considers pitfalls in document management, and also provides a number of helpful tips and techniques to help in managing and securing documents and content, and making them easier to find when you need them — even years down the road.
Digital Hygiene: IAM – Internet Authentication Method a.k.a. Identification

Authentication and Management Parts I & II — Through wireless networking in particular, the Internet has truly become a ubiquitous and firmly entrenched element of global culture and commerce. While this ubiquity engages us and enables communication and industry, it has also created numerous new threats to our physical safety and that of our personal identities. It seems that every day, the news media bring new stories of abductions or near abductions of children, or losses of personal data from improperly stored hard drives, or even voter fraud made possible by computer code hiding within mysterious black boxes. In a discussion that is sure to raise objections and controversy, this article will present a comprehensive, albeit imperfect, solution to many of the problems created by our new world of global networking. IAM is a proposed scheme to simplify user authentication and personal data security while providing strong protection against criminal activity including protection from fraud and prevention of child abuse online.

This entry was posted in Uncategorized by Editor. Bookmark the permalink [http://bcis.pacificu.edu/interface/?p=3276].

4 THOUGHTS ON “DIGITAL HYGIENE: CLEAN LIVING ON A DIRTY NETWORK”

dating online
on February 3, 2014 at 1:43 AM said:

I do enjoy visiting your website, you often make me suprise with great articles.

temat
on February 3, 2014 at 1:56 AM said:

Hi Shane, I’ve very appreciated these content as well as the helpful summaries that they provide. You say both “the Son is God” and suggest we shouldn’t say “God died on the cross.” Can you explain? Thanks!

naija
on February 4, 2014 at 10:18 AM said:

Hello, you utilized to write good articles, but the last several content were kinda boring...
I miss your great articles. Past quite a few content are just a tiny out of track!
nigeria entertainment news

on February 4, 2014 at 10:39 AM said:

If you are going away to watch comic videos on-line then I suggest you to pay a quick visit this site, it consists of genuinely thus comical not only movies but also far more data.