THE NAVIGATOR
COMPASS
NETWORK GROUP

July 2016

Hacker Lexicon: What Are CNE and CNA?

Doing Less To Get More Done

Control What People See When They Google Your Company

Do You Cover Your Computer Camera? You Probably Should.

SERVICE HIGHLIGHT: VoIP Services

Hacker Lexicon: What Are CNE and CNA?

In today's digital world, espionage looks much different than it was during the Cold War.

Modern operations of electronic espionage use computer networks to infiltrate target or adversary automated systems and networks and steal data or obtain intelligence. These techniques and processes are known as Computer Network Exploitation, or CNE.

Primarily used within military institutes and organizations, CNE examples include Flame, a huge spy tool used to gather intelligence from Iran and other targets, and Regin, used to hack the European Commission and Belgium's partially state-owned telecom Belgacom.

CNA stands for Computer Network Attack, operations designed to damage, destroy, or disrupt computers or networks.

An example of CNA would be the Stuxnet attack that targeted centrifuges used by Iran to enrich uranium hexafluoride gas, or the air-to-ground hack conducted by Israel in 2007 against Syria's air defense system, and

the recent hack of power distribution plants in Ukraine.

Many CNA operations begin as CNE, best illustrated by the hack of Sony, attributed to North Korea, when the hackers extracted data from the company's network first and then destroyed data and systems.

Per 2011 EU cyber security policy document, "...technically speaking, CNA requires CNE to be effective. In other words, what may be preparations for cyber-warfare can well be cyber-espionage initially or simply be disguised as such".

Both CNE and CAN are part of Computer Network Operation (CNO) - a comprehensive military and civilian computing concept that involves tools, processes and methodologies to employ, optimize and gain strategic advantages from computer networks.

CNE and CAN can also be used to target businesses, which means you need to protect yourself and your sensitive information.

READ MORE

Control What People See When They Google Your Company

You optimize your site for certain keywords so you can get organic results, based on your brand or industry. However, you also want to be able to provide more information to your users and be a greater authority in your industry.

Here's how you can promote your brand and increase your search visibility:

1. Distinctions and Variables
Mention your brand name throughout your site as appropriate, link to your home page, and optimize in your title tags and meta descriptions.

2. Expanded Site Links
Set up your site navigation methodically, include your most important pages, and write descriptive titles and meta descriptions for each.

Then, leave it to Google - the more branded search traffic your brand has, the better, so engage in a content-marketing strategy to grow your brand.

3. Social Media Profiles
Your social media profiles will likely show up in your branded-search results - claim all your major ones, fill in as much info, and link them to and from your website.

4. Knowledge Graph Entries
The Knowledge Graph pulls information most significantly from your own website. Tell Google which info is most pertinent and categorize it, and claim as many local citations, and optimize your company's reviews.

5. Google Reviews
Make sure your earned Google reviews are in good shape, as they may help you earn a boost in organic search rankings and help establish you among branded searchers.

So, set up and claim your profile on Google My Business, then encourage your top customers to leave detailed reviews from their Google accounts.

6. Branded Articles
One of the best ways to fill the space on page 1 of the search results with positive results is through branded articles, which you can publish offsite.

The key is to use your company's brand name in the headline.

7. Link To Your Most Desirable Results
Build links to your favorite results! You may also consider building more links to your most important main navigation pages.

Take all these steps to ensure that your online properties are the first to show up for any branded search, and to make the best impression possible for new and returning searchers.

READ MORE

Doing Less To Get More Done

If you're a fan and a believer of multitasking, think again.

Turns out, multitasking is counter-productive - not only is it not nearly as efficient as we like to believe, but research shows that it can even be harmful to our health. It doesn't work for individuals, and it doesn't work for teams; and, it doesn't work for leaders of teams.

If you want to get more done faster and better, do things consecutively rather then in parallel.

The data to support this keeps getting stronger and stronger. Studies from the Universities of Utah, California, Western Washington, Essex, Illinois, and France revealed that when we focus on one task at a time, we are faster, more productive and more creative, remember more with less mistakes, and less stressed.

So, most of the hype and hacks about productivity are old news. Multitasking is really only task-switching, explains Guy Winch, PhD.

And the emerging trend may surprise you - doing nothing is a new productivity trick.

Psychiatrist Samantha Boardman shared that more and more of her patients are struggling to do nothing, and that downtime is, for many people, challenging.

Boardman cites studies that show that "solitude is associated with freedom, creativity, intimacy, and spirituality".

Doing nothing is one of the activities psychologists call incubation, which helps you solve insight problems. Just being with our own thoughts regularly is essential for creativity and self-definition.

So for good health and productivity - do less at a time, and make time for downtime.

Do You Cover Your Computer Camera? You Probably Should.

As more businesses use webcams to conduct webinars and videoconferences, and more people use the webcam for Skype and other chat platforms - a new security issue has surfaced.

We learned that FBI Director James Comey covers his webcam with a "piece of tape". Recently Mark Zuckerberg revealed that he also tapes over his webcam.

So, what are your thoughts on this little, yet powerful, circular lens?

Webcams are in itself a great invention – they allow us stay in touch with friends and family. The issue is - hackers could access your webcam and remotely record video or photos, even stream on a publicly accessible website.

Recently, a school district in PA was accused of using webcams on school-issued laptops to spy on students and their families, while a sophisticated network of hackers in China known as GhostNet has hacked 1,295 webcams in 103 countries.

IT security expert Steven Fox, who writes a column for the journal of the Information Systems Security Association and whose own webcam had been hacked one night while chatting with a friend, warns people to pay attention to the indicator lights that flash when their web cameras are on, and to avoid storing camera-equipped laptops in private areas like bedrooms.

As most laptops nowadays have a built-in webcam, understanding the risks is vital.

Most hackers use a malware called Trojan, says Richard Stiennon, a malware expert with IT-Harvest, a research firm that specializes in Internet security. If you click on an attachment or download a piece of music or video that's infected with a virus, a hacker could remotely control your PC's functions.

The good news is – you can take steps to secure your webcam, and here are some key things to keep in mind:

- Don't click on suspicious attachments (such as those in funny emails forwarded by friends and family), or links on sites offering free downloads of music, TV shows or videos.

- Use a firewall - your computer comes with one, but make sure it's turned on.

- Use robust anti-virus software - install a security suite that offers malware and spyware protection.

- Don't keep PCs with webcams in bedrooms, and don't do anything in front of a webcam that you wouldn't want the world to see.

- Secure your wireless connection - make sure it's protected with a unique password (not the default one that came with the router).

- Avoid IM chats with people you don't know. Make sure your kids do the same.

- Be cautious about accepting tech help - hackers have been offering computer help in order to rig webcams and spy on the computer user.

- Observe the indicator light - a red light on external webcams and a blue LED on laptops with internal webcams indicate the camera is on. Detach an external webcam from the USB port when not in use.

- Finally, simply cover the webcam lens - with a lens cover, an adhesive bandage, or a sticky note, making sure nothing sticky touches the lens.

SERVICE HIGHLIGHT: VoIP Services

If you have traditional POTS (Plain Old Telephone Service) or onsite PBX (Private Branch Exchange), you can benefit greatly from our cloud based VoIP phone services. Voice over Internet Protocol, or VoIP, is a technology allows delivery of voice communications and multimedia sessions using a broadband Internet connection.

For more information about our VoIP services, our proficient techs are here to assist you.

Navigate to better dentistry-specific technology - call Compass Network Group, Inc. today: (866) 336-8727.

What do you get with VoIP Services by Compass Network Group?

- Many more features than with POTS, such as limitless call routing, without the upkeep of traditional PBX systems

- Easy to use and operate

- Improved scalability

- Flexible and future proof - access from anywhere in the world

- Save money upfront - no heavy investments to get started

- Save money over time - lower your monthly phone bills

- We typically match or beat providers like Comcast

- One point of contact for all of your technical support needs.