Practitioner Perspectives

WOLF DEN ASSOCIATES, LLC

August 2014 *(Vol. 3; Issue 8)*

10 Tips From Your Technology Trackers

1. ***Lock down privacy settings and scrutinize inbound traffic on social media sites***
2. ***Maintain the most updated versions of OS and software***
3. ***Do not install Java or Flash unless absolutely necessary and consider uninstalling immediately after***
4. ***Disable cache cookies before browsing the Internet***
5. ***Protect passwords and use different passwords to safeguard sensitive sites***
6. ***Home users should consider employing a virtual machine for PII-intense activities***
7. ***Establish clear social media policies and monitor compliance against them***
8. ***Create an air gap between corporate infrastructure and the Internet***
9. ***Separate guest networks from office networks***
10. ***Segregate work material from personal computers and smart phones unless they maintain the same security standards as office workstations***

Naked and Afraid: In the Cyber Serengeti

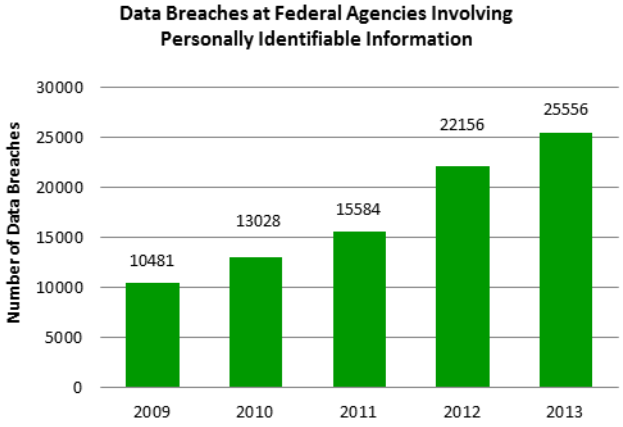
- The Internet's function as the *de facto* social hub has created a windfall of easily exploitable personal information
- The advent of cloud storage and high speed networks have ushered in the Golden Age of Sharing and also the Golden Age of Espionage
- "Digital dandruff" creates a trail of breadcrumbs bad actors are using to mount increasingly sophisticated and targeted attacks
- While most users are aware that threats exist on the Internet, they have not modified their behavior to minimize their vulnerability
- Running naked through the Cyber Serengeti is like secondhand smoke – not only do you endanger yourself, but also everyone around you
- To minimize corporate liability, focus at least as much on policy and continuous monitoring of user behavior as on network defense

Gathering at the Watering Hole

The Internet has become a ubiquitous digital watering hole. Originally a tool for researchers and fault-tolerant communications, it now permeates every facet of our lives. Email, calendars, document storage, photo archives, banking, shopping, dating, voice communications, entertainment, and navigation have collided in cyber space – at home, at work, and on the go. As people traverse this wild binary frontier, they leave behind bits of "digital dandruff." Most of these traces are innocuous, but some have the potential for disastrous effects. With treasure troves of personal data available, bad actors can easily assemble profiles that can be used to answer security questions, change passwords on banking sites, and ultimately steal identities.

Digital Hyenas

Online information sharing makes it easier than ever for bad actors to pick off the weakest members of the herd. No special tools are needed, people of all ages participate, and – as The Internet of Things propagates – the attack vectors for the next generation of script kiddies grow even broader. This is not the Orwellian scenario over which the tinfoil hat set obsesses, this is real. Whether it is a DOS attack on home appliances (the bored teenager across the street correctly guesses the password is a pet's name) or a remote disarming of home security systems (just after Facebook posts from overseas), personal attacks such as these become more feasible the more inter-connected the world becomes. Highly sinister attacks parlay information stolen from these vectors to glean more valuable information from friends and co-workers en route to the big game trophy – accessing corporate networks and data marts.



While the pace of growth has slowed, data breaches at Federal Agencies involving PII still occur at an average rate of 100 breaches per day.

Source: GAO-14-487T

Stalking the Prey

Within the cyber landscape, the weak endanger the entire herd. Patient attackers lay low, stalk their prey, and quietly collect enough Personally Identifiable Information (PII) to go in for the kill. The Instagram pictures posted from the parking lot of an office building are just a few LinkedIn connections and a pipl.com search away from a spearphishing attack on a co-worker that inadvertently gives up network access credentials. This sets into motion a virtuous cycle of PII arbitrage whereby attackers can expand horizontally to additional co-workers (small potatoes) and mount increasingly vertical attacks that penetrate deeper into an organization, syphoning off trade secrets and customer information in a digital feeding frenzy.

Circle the Herd

As attacks grow in severity from pranks and inconveniences to major corporate data security breaches, companies need to circle the herd to protect the weak and fend off the hunters. While there have been several recent high profile cases of corporate data breaches, these barely scratch the surface. Far more network compromises are reported to US-CERT than find their way into the press. This is due in part because of public relations concerns, and in part because of the desire to observe bad actors before they know they have been caught. For companies that operate in the federal sector, the stakes are particularly high. From the FAR definition of "information security" to recent amendments to DFARS Parts 204 and 252, federal contractors face potential work stoppages, terminations for convenience, fines, and civil penalties for breaches. This is no longer a matter of trading convenience for security, it is a matter of corporate survival.

8280 Greensboro Drive
McLean, VA 22102
wolfdenassociates.com

Rick Tossavainen
(703) 638-5924
rick@wolfdenassociates.com

John Shellhouse
(301) 356-1027
rambo@wolfdenassociates.com

Martin Bonica
(703) 678-6296
martin@wolfdenassociates.com