Open Feedback Dialog
Random Article

- NEWSLETTER
- CONTACT US
- ADVERTISE
-

unlimited
EXPAND YOUR LIFE'S WORK

Search

- Work /
- Money /
- Know-How /
- Personal Best /
- Management /
- Blogs /
- Multimedia /

FRIDAY, AUGUST 12

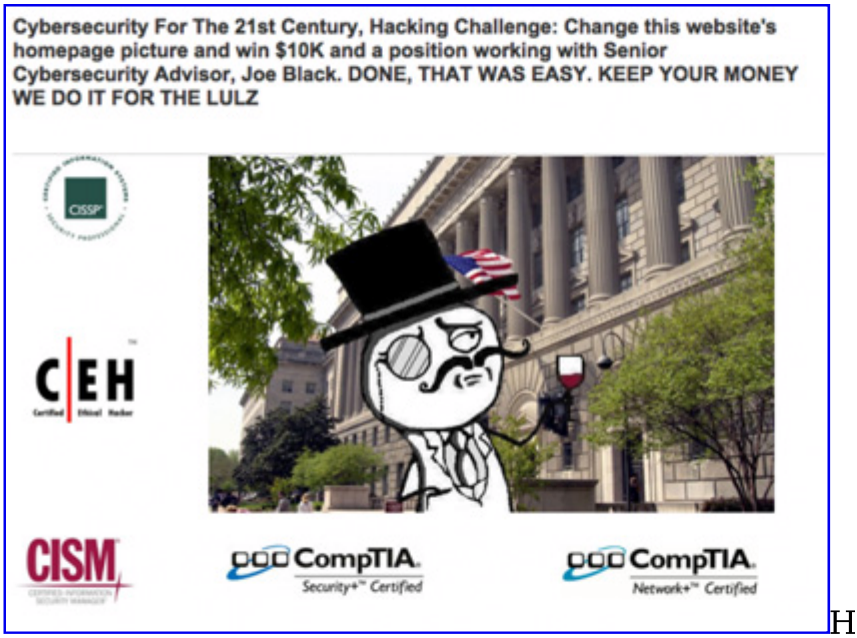
Spy vs Spy

What you need to know about the Sisyphean struggle between hackers and their opponents

SHARE

Like Sign Up to see what your friends like.

By Lewis Kelly



Cybersecurity For The 21st Century, Hacking Challenge: Change this website's homepage picture and win $10K and a position working with Senior Cybersecurity Advisor, Joe Black. DONE, THAT WAS EASY. KEEP YOUR MONEY WE DO IT FOR THE LULZ

Has Sony been hacked this week?

Odds are pretty good the answer is “yes.” Earlier this summer Sony suffered 20 hacks in 60 days. The blog HasSonyBeenHackedThisWeek.com tracks the ongoing and evidently futile struggles of the multinational electronics giant against online intruders.

At least Sony doesn’t stand alone in that regard – the list of those recently hacked runs from Bethesda and BioWare to the U.S. Senate, Bank of America and the C.I.A.

On top of more conventional signs of the apocalypse like volcanic eruptions and earthquakes and Rebecca Black, 2011 has been filled with more high-profile hacks than a *News of the World* office party. No one, not even digital security firms like HBGary and RSA, can protect themselves.

What gives? Widespread Internet use began over a decade ago and digital security consultants started getting work even before then. Why can’t anyone, even self-described security experts, keep online criminals out of their business?

“Anyone who says you are secure is lying,” says Brad Haines. “They just haven’t found the holes yet.”

Haines, who goes by the handle “Renderman” online, works as a computer security consultant in Edmonton. He describes digital security as an arms race with the advantage perpetually granted to the attackers. “The technical skills are a lot harder on the defense side,” he says. “You have to be right every time. The attackers only have to be right once.”

Haines makes it his business to be right every time – he even relishes it. “I take it as a personal challenge when I’m securing a system,” he says. “I’m always thinking about it.” Not that he expects he’ll never be hacked, but he’s good enough to make his living keeping unscrupulous web surfers out of places they shouldn’t be.

Kevin Cardwell, a former member of the U.S. Navy turned computer security consultant, also points to the inevitability of getting hacked. “Given time and resources,” he says, “I can crack anything.”

Cardwell, whose clients include the government of Oman, leads teams around the world that practice the digital equivalent of testing your house’s security by paying thieves to try to break in. “You use exactly the same tools, motives, techniques, everything that the malicious hacker does,” he says. “The only difference is you get authorization and permission in writing to go and carry out the attack.” Theoretically, this identifies the gaps in a security system, allowing them to get plugged before someone makes off with company emails or security keys.

Both Cardwell and Haines demonstrate the feasibility of using precisely the same skills others employ to pull pranks and steal information to make a legitimate living. They differ in their educational backgrounds: Haines is self-taught while Cardwell holds an M.Sc. in software engineering and lists an alphabet soup of acronyms on his biography like LCFE (Live Computer Forensics Expert) and QPT (Qualified Penetration Tester).

Cardwell also teaches others to think like hackers at EC-Council University. The online school offers a Master of Security Science degree that purports to prepare students for careers preventing hackers from achieving their aims. A variety of schools like New Horizons and Secure Ninja offer similar training for aspiring Dade Murphys who don’t have the time or inclination to teach themselves.

But Cardwell admits that these schools don’t provide an iron-clad guarantee of comprehensive knowledge. “The security community is terrible,” he says. “The hacking world has been much better at communicating and sharing information than we have.”

And as Haines argues, in online security the proof of the pudding ultimately lies in not letting anyone else make off with said pudding.

“You’re 100 milliseconds away from every jackass on the planet when you’re on the Internet,” he says. “You have three billion pairs of eyes looking for any sort of hole. That’s frightening and cool at the same time.”

Both Haines and Cardwell say that digital security requires thinking like a hacker. “You need to understand the attacker – not just the tools, but the mindset,” says Haines.

Out-thinking every jackass with Internet access is a tall order – one even specialists in the field can’t always meet. Witness Black and Berg Cybersecurity Consulting. The California-based firm, which bills itself as “Home of America’s Private Sector Cyber Command,” challenged hackers with a contest — whoever defaced Black and Berg’s homepage first would win $10,000 and a job with the company. Infamous hacker collective LulzSec appended “DONE, THAT WAS EASY. KEEP THE MONEY, WE DO IT FOR THE LULZ” to the contest posting shortly after.

But despite the impunity with which hackers seem to dance around so many security measures, Cardwell says a modern computer, regularly updated, does a pretty good job of keeping hackers out – provided, of course, that the user remains vigilant about where they stick their cursor. “Unless someone turns something on or clicks on something, it’s hard to hack ‘em,” he says.

People, of course, do click things and turn them on from time to time. In an age of endless passwords and security approval screens, the temptation to use the same password for multiple accounts and blindly click “yes” when your computer asks for your permission can prove too much for many, including those who should know better. The hack of security firm RSA started when an employee clicked on an Excel file attached to an email.

“People need a better bullshit filter,” says Haines. “If it’s too good to be true, it probably is. Always assume the other guy is out to screw you.”

The more people fail to make that assumption, the more high-profile hacks will take place — and the more the public notices its vulnerability, the more business ultimately winds up at the door of people like Haines and Cardwell. And while asking a digital security consultant if people pay enough attention to hacking is a bit like asking a general if the defense budget is big enough, it’s tough not to feel that the profile of hackers and those who try to stop them will only increase in the future. “The problem we have today is that information on the Internet never goes away,” says Cardwell.

“It’s always out there and we can grab it.”

Share this on

Category: Work Tags: hackers, hacking, internet security, LULZSEC

- Digg
- Stumble Upon
- Buzz Up!
- del.icio.us
- Facebook
- Twitter

This entry was posted on Monday, August 1st, 2011 at 12:09 am and is filed under Work. You can follow any responses to this entry through the RSS 2.0 feed. You can leave a response, or trackback from your own site.

Leave a Reply

Name (required)

Mail (will not be published) (required)

Website

Submit Comment

- MOST READ
- MOST RECENT
- COMMENTS

MOST READ

// Three Unconventional Self Help Techniques
These aren't your grandma's self-help tips, these are from the fringes of economics, psychology and common sense

// How Less Can Be More
Happier living through minimalism

// Personal Best: Unlimited's New Style and Etiquette Column
Meet Miranda Wulf, your guide through this oft tricky subject

// Strange Brew

Don't believe the cleanse hype

// Get Out of Town
Why you need to move away

MOST RECENT

// Personal Best: Digital Decorum
What you text can and will be used against you

// Job on a Wire
Telecommuting is becoming increasingly popular, but do you have what it takes to be productive in your pyjamas?

// Book Review: You Are Not A Gadget
Organizing a different digital world

// How to Create a Tech Cluster in Oil Country
Turns out you really shouldn’t mess with Texas

// The Evolution of Procrastination
How and why we sabotage ourselves

COMMENTS

Cailynn Klingbeil on How To Create An iPhone App.

Vlad on How To Create An iPhone App.

Candice on How To Create An iPhone App.

Michelle on The Evolution of Procrastination.

jotbuzz.com on How To Create An iPhone App.

Lim Thye Chean on How To Create An iPhone App.

Marcus Hast on How To Create An iPhone App.

Andrew on How To Create An iPhone App.

Paul Joslin on How To Create An iPhone App.

Michael Langford on How To Create An iPhone App.

Editor’s Pick

Job Training

July 01, 2011 / 1:21 am

Laura Trethewey hopped a train from Toronto to Vancouver, stopping in cities along the way to talk with regular Gen Y-ers about their jobs. Take a look at Job Training, our interactive map to read her profiles, which are being added weekly.

> Read More

Related Reading

+ No Related Post

- **Newsletter**

*Sign up to receive the latest Unlimited news and business tips in your inbox.

enter your email

Go

Unlimited Archives | Venture Publishing | Advertise | Alberta Venture | Think Alberta | Contact | Masthead | Contributors | Privacy