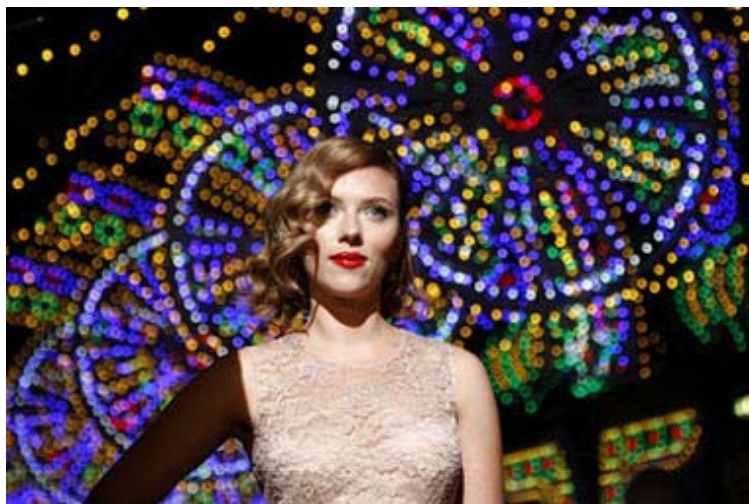


The Christian Science Monitor - CSMonitor.com

Scarlett Johansson cellphone pictures aren't all that smart phone hackers are after

As more and more corporate and personal business is done via mobile devices and social media, it is more than Scarlett Johansson cell phone pictures that are being hacked.



Actress Scarlett Johansson poses for photographers on the catwalk before the Dolce & Gabbana Spring/Summer 2012 women's collection during Milan Fashion Week September, 2011. Ms. Johansson's mobile phone was hacked in September. (Alessandro Garofalo/ REUTERS)

By [Gloria Goodale](#), Staff writer
posted September 30, 2011 at 12:43 pm EDT

Los Angeles

Cellphone hacking has had more than its 15 minutes of fame recently, from the [London](#) reporting scandal that shook [Rupert Murdoch's](#) media empire to the recent complaints from Hollywood celebrities [Scarlett Johansson](#) and [Mila Kunis](#) that private photos were stolen from their mobile hand-helds.

But these are not just isolated headlines, says former hacker [Kevin Mahaffey](#), now chief technology officer for [Lookout Mobile Security](#). The trend is accelerating quickly, he says.

"Just from January to June, the likelihood of a mobile malware attack has gone up 2-1/2 times," he says, citing a recently released study by his firm. Computing is moving from desktops to mobile devices, he says, and as it does, so will serious hacking activity.

RECOMMENDED: [Data theft: Top 5 most expensive data breaches](#)

Hacker [Kevin Mitnick](#) is eager to show how easily anyone can be hit.

"Give me your cellphone number," he says in an interview. Within seconds he has sent a spoof text message to my co-worker's cellphone, as if it were coming from my number.

It appears I am telling her, "Please go to this site, ASAP – [stackoverflow.com](#)."

This is a classic ruse, Mr. Mitnick says, pointing out that a malicious hacker would have inserted a booby-trapped website that could then mine passwords and other personal information from my friend.

"Because she trusts you, she probably would click on the link without worrying that it might be fake," says Mitnick, a once-notorious hacker who spent five years in federal prison for his crimes. He now travels the globe teaching Fortune 500 companies how to keep their information safe.

This illustration underlines a sobering reality in an increasingly mobile, social media-driven daily life, say Mitnick and fellow security and technology experts: As more and more corporate and personal business is done via mobile devices and social media, consciousness about security in the new environment is not keeping pace.

RECOMMENDED: [Hackers rally to support WikiLeaks: Top 5 recent attacks](#)

Technology moves faster than we do, says [Harry Sverdlove](#), chief technology officer for [Bit9](#), an Internet security firm based in [Waltham, Mass.](#) "Technology itself progresses at the speed of electronics," but the way society uses new tools and understands the pitfalls of them tends to progress at a much more human pace, he adds.

In the rush to embrace new technologies, "we shed precautions learned with previous technology like so many old clothes," he says. A survey earlier this year by Trusteer, a financial services security firm, revealed that people were three times more likely to click on an unfamiliar link sent to their cellphone than one received on their desktop computer.

"People have very different attitudes about their cellphones than they do about their computers," says [Ben Knieff](#), director of fraud management technology at NICE [Actimize](#), which specializes in security services. Mobile phones have a very personal, private feel to them, he adds.

"It's psychologically very different from the computer they know," says [Joseph Steinberg](#), chief executive officer of Green Armor Solutions, a security software company, "because phones are in your pocket and feel very intimate." But what many users fail to realize is that today's sophisticated smart phone technology has converted these pocket devices into complex computing and Internet communications machines with a secondary phone functionality.

"Folks still don't realize that their smart phone is really a small computer," says [Jack Walsh](#), program manager for [International Computer Security Association Labs](#), which certifies security applications. "Mobile phones today have more computing power than all of [NASA](#) in 1969," he says via e-mail.

And, he points out, even the battle to engage average computer users with basic security safeguards such as hard-to-guess passwords and robust antivirus software is far from won. "Heck," he adds, "folks are still having trouble understanding that they have to use caution when using their desktops and laptops! So, it will be a while before they realize their phone has to be used with caution."

But while consumers and even corporations have been slow to take mobile and social media threats seriously, hacking has become serious business, says [David Koretz](#), CEO of Mykonos Software.

"Hacking is exploding because the underlying motivations for hacking have changed," he says via e-mail. The old image of a hacker as a pale, brilliant American kid living in his parents' basement and taking over missile-control systems is gone. The reality couldn't be further from that old myth, he says.

"Today's hackers are sophisticated organized crime syndicates stealing billions of dollars, rogue activists stealing damning political information, and nation-states stealing classified data," he says. "They are smart, organized, and well financed."

Mitnick, whose book "Ghost in the Wires" details his exploits as a hacker on the wrong side of the law, says the spoof text message demo is one of his favorites because it shows the importance of tackling the human component of hacking.

In two highly publicized recent attacks on corporate [Twitter](#) accounts at [Fox](#) and [NBC](#), intruders sent phony tweets to cellphones and other followers. The intruders gained access by tricking employees into revealing their company passwords, a practice known as social engineering.

These are extremely low-tech gambits that rely on human foibles, not complicated machinery.

"That is really the largest threat to security," says [Chris Hadnagy](#), author of "Social Engineering: The Art of Human Hacking." He points to an interview with a member of Anonymous, the global hacking coalition.

"This guy said every hacking attack they've ever launched involved some element of social engineering," he says. Systems are getting more secure all the time, but no system will ever be foolproof against human error. "Nothing," he says, "can replace critical thinking."

[QUIZ: Could you pass a US citizenship test?](#)

Get daily or weekly updates from [CSMonitor.com](#) delivered to your inbox. [Sign up today.](#)



The advertisement banner features a blue background with a subtle pattern. On the left is the Pardot logo. The main text reads 'Automate your lead scoring and nurturing in' followed by 'a white paper >'. To the right, a white box contains the text '4 Quick Steps' with a 'FREE' tag above it. Further right is an orange 'Download Now!' button. A small 'AdChoices' icon is in the top right corner.

Pardot

Automate your lead scoring
and nurturing in
a white paper >

4 Quick Steps FREE

Download Now!

© The Christian Science Monitor. All Rights Reserved. [Terms](#) under which this service is provided to you. [Privacy Policy](#).