

MALWARE AND PRIVACY

STAYING SAFE IN A CONNECTED DIGITAL WORLD

Nobody is immune from the effects of malware. It is pervasive and stealing more than online banking credentials. When installed, malware is capable of capturing everything a user does and gaining full access to a device. Whether at home or at work, it's everyone's job to ensure online safety.

Here is a small sample of the astounding finds RSA uncovered stolen by financial malware.

Online Dating

On a popular online dating website, users are allowed to pose questions to a potential date. One suitor asked, "As a former employee of the government, is there anything in your past I should know about?"

Attention All Burglars

Malware captured the following message that was sent by one online user: "When you come into the house, enter this alarm code into the keypad." Enough said.

Password Strength

A popular virtual gaming website was offering a trial for new gamers. One online user applied, and selected "nightmare" as his password, but it wasn't strong enough. He then selected "nightmare8" and was advised by the site that it still wasn't strong enough. So he selected "nightmare89" which the site indicated was "strong." Not that strong when the malware on his computer captured all three passwords.

Political Activism

Malware captured the message of one activist U.S. citizen who wrote to his Senator: "Do you really think this is what needs to be done? You morons in the government need to get a clue. I am taxed enough as it is. This is nothing more than highway robbery!!!!"

Housing Benefit Fraud

Malware captured an anonymous complaint filed on a government website that stated a certain Mrs. Fields "receives housing benefits and doesn't pass it on to the owners of the property!" Mrs. Fields is slim, has tidy blonde hair and drives a silver Land Rover, said the anonymous report. Did we say anonymous? Well, not really considering the report was filed from Mrs. Field's laptop.

Unhappy Rich

An employee at a large IT company recently shared with a friend that he was less than thrilled about his recent transfer to Europe. How do we know? Because the Trojan on his computer stole the following email: "I have a Ford Focus. It's very small. In fact, everything here is small. The gas is \$7/gallon. My corporate VPN just crashed and I cannot get anywhere on the corporate network."

Consulting

A large manufacturing company was in the process of changing its ERP systems. They hired a consultant to run the project. One of the internal memos within the consulting firm read: "We are being asked to evaluate the following five criteria. I can do the first four, but I have no clue about the fifth, it's rather stupid. What do you suggest we do?" One suggestion: Do not discuss customer projects from a computer infected with malware.

Job Seekers

An employee of a large aerospace company was infected with malware which stole his Protected Storage (why on earth is it called protected?) - including his access codes to the company where he works. The next entry in the Protected Storage was the access codes to jobs at his company's biggest competitor. Someone is looking for a new job.

Corporate Financial Records

An employee of a global company that was working overseas received an email from the headquarters of his parent company based in the U.S. The subject line of the email: "Sales projections and profit plans." Attached was an Excel spreadsheet with every bit of information you would want to know about before deciding to invest in the company.

Nobody is immune from the risks of malware. To learn more, visit: rsa.com