Hackers are going after your online bank account

By Brooke Crothers, Fox News

April 19, 2018 | 2:58pm | Updated

iStockphoto

ORIGINALLY PUBLISHED BY:

FOX NEWS

Feds: Russian cyber spies exploiting unpatched routers

Senate cracks down on election hacking, pushes bills to protect the vote

Your online identity sells for exactly $1,170 on the dark web

Banking and finance sites have the greatest risk for getting hacked, a new report says.

The worst vulnerabilities were found in banking and finance web applications tested by Positive Technologies, a firm that provides internet security products for businesses.

“Greater complexity results in more opportunities” for hackers, according to the Positive Technologies report, which said banking applications are some of the most complex.

The hackers primary target is the average user. “The number-one threat is attacks that target web application users,” the report said. A whopping 87 percent of banking web applications tested by Positive Technologies were susceptible to these attacks.

Government app users are also big targets because they tend to be less security-savvy, making them easy victims, the said.

“We gained access to personal data of 20 percent of the applications that process user information, including bank and government websites,” the report added.

The most common vulnerability was Cross-Site Scripting, which allows attackers to perform phishing attacks, which can result in malware infection. In a phishing attack, the hacker sends, for instance, an email pretending to be a trusted entity like a bank or major shopping site, hoping to dupe you into clicking on the malicious link.

Denial of service (DOS) attacks – which block access to a website or service – are common. In 75 percent of e-commerce web applications, there are vulnerabilities enabling DoS attacks, Positive Technologies said.

“Denial of service is especially threatening…High-profile e-commerce web applications receive large amounts of daily visits, increasing the motivation for attackers to find vulnerabilities to turn against users,” the report said.

Employees are weak links

In a separate report released earlier this month, Positive Technologies said employees are often the gateway for attacks.

An alarmingly high percentage of employees download malicious files, click phishing links and even correspond with hackers, the report said.

Positive Technologies testers pretended to be hackers by sending emails to employees with links to websites or forms that required password entry, the report said. Of the 3,332 messages sent, 17 percent of these messages would have led to a compromise of the employee’s computer and possibly, the entire company.

The most effective method was to send an email with a phishing link. In that case, 27 percent of recipients clicked on the link. “Users often glance over or ignore the address, leaving them unaware that they are visiting a fake website,” the report said.