Increasing numbers of consumers are browsing and making their purchases online, and are clearly embracing e-commerce with 200 million online shoppers in the U.S. spending nearly $600 billion.

The results of a new survey commissioned by the CA Security Council (CASC) found that consumers understand online security but lack the attentiveness to certain aspects of it.

Overview

After years of belt tightening brought on by the Great Recession of 2007, Americans’ optimism for the economy’s recovery is rising, accompanied by a soundtrack of ringing cash registers and computer mouse clicks. More Americans are shopping again, with six in 10 people telling Consumer Reports that in 2014 they had spent money on a major purchase such as an appliance or a car.¹

Increasing numbers of consumers are browsing and making their purchases online, and are clearly embracing e-commerce with 200 million online shoppers in the U.S. spending nearly $600 billion. This number continues to rise despite the rash of news headlines about data breaches at some of the world’s largest retailers and financial services institutions. This implies that consumers have a good understanding of, and trust in, the security of the online e-commerce infrastructure.

The results of a new survey commissioned by the CA Security Council (CASC) found that consumers understand online security but lack the attentiveness to certain aspects of it. These findings present an opportunity for those who do business online to educate consumers better so they can avoid risky behaviors. They can also serve as a lesson to retailers, financial institutions, and others about why taking the necessary steps to earn a green bar and a small padlock symbol next to their website URL addresses can increase the security of the site and attract new customers.
Key Findings

First, consumers want the highest level of protection available and they recognize that the padlock and green bar provide a trusted connection. In this study, we found that the padlock and warnings do appear to work. Just two percent admit to ignoring the “untrusted connection” message, and only three percent would give out their credit card information to sites without the padlock icon. Thus, the padlock symbol is something consumers actively look for, even if they don’t understand how the SSL validation process works or what assurances they can assume.

The study also confirmed that consumers find online shopping to be important. While shopping in person at a consumers’ store still leads in terms of total spending, online shopping represents more than a third of consumers’ budgets (38 percent).

This mirrors the findings of similar studies conducted by retail industry watchers. For example in February 2015, E-commerce Platforms and Forrester Research released a joint report predicting that e-commerce sales in the U.S., which totaled $176 billion in 2010, will rise to $279 billion by the end of 2015.

What was surprising was consumers’ attentiveness toward certain aspects of online security, especially considering 100 percent of them had either fallen victim to cybercrime, or knew friends and family members who had. These incidents include compromised passwords, identity theft, lost or stolen computing devices, hacked online accounts, and stolen personal items or photos.

Despite being well aware of the risks, consumers need to be more attentive to overall security issues. Most reported to have at least one device they don’t bother password protecting. The most common device left unguarded is the tablet, a device that 61 percent leave unprotected. Forty-three percent are happy to use Wi-Fi without regard to security issues, as long as it is free. Finally, 33 percent use just one or two passwords to login across all their websites. This is especially problematic when considering the number of companies experiencing breaches that resulted in stolen passwords within the last few years.

**METHODOLOGY:** The CA Security Council recently commissioned Survata Consumer Research to survey 670 U.S. consumers to gauge how security savvy they really are, and how much they trust the e-commerce infrastructure. Survey respondents were 18 years or older and shopped at least several times each year.
However, consumers do appear to have taken the time to educate themselves about how to identify secure e-commerce sites and to avoid those that pose greater risks to their information and interactions. The majority are somewhat savvy about SSL security: they recognize the padlock symbol in their browsers’ URL address bars, and understand that the padlock and the green bar keep them safe. They just don’t understand how.

EV-SSL certificates use the highest level of authentication and indicate a rigorous verification process. Sites with EV-SSL certificates provide visual cues such as the green bar in a browser’s URL. Consumers know to favor websites that display the padlock symbol and the green bar in the URL, but they could still benefit from greater education on how certificates work, the benefits of authentication, and to highlight why EV provides value to businesses and consumers. Better educated consumers are not only less likely to fall victim to cyber thieves, but they are more likely to help their friends and family adopt conscientious behaviors too.

A final survey question dealt with who consumers trust the most and least to keep them safe from financial or privacy threats while shopping online. Financial institutions scored highest followed by certificate authorities at 49 percent. This finding points to a need to educate consumers on the work CAs do on their behalf and to draw the direct line between the padlock symbol they see in their browsers and the role CAs play in determining when a site has earned the right to display that symbol.

This also helps explain why consumers look for the padlock and the green bar. Without it, they are left to trust the online merchant exclusively, and only 40 percent are comfortable with that. So, the lesson for retailers is this: Add a padlock and a green bar and you will draw a larger share of the more than 200 million Americans who are spending nearly $600 billion online.
Retailers trying to build up their e-commerce operations must realize consumers will not visit unless they trust them to protect their private information.

The security industry and CAs are a powerful tandem to ensuring retailers earn consumers’ trust by enforcing the highest standards for identity vetting prior to issuing certificates.

Recommendations:

These findings point to five best practices consumers should follow to keep their information safe:

1. Update your browser to the latest version, which addresses the most current online risks.

2. Look for “https” in the address bar. The “s” means it’s secure. You should also see a padlock symbol. For an added sign that the site is authentic, look for the green browser bar and the website’s name to appear in green.

3. If your browser gives you a message about an untrusted security certificate for a website, don’t proceed.

4. Wherever possible, don’t allow merchants to keep your payment information on file.

5. Regulated industries and e-commerce should use high validation to provide stronger trust and assurance to customers and to protect against fraud.

The responsibility does not rest with consumers alone. Retailers trying to build up their e-commerce operations must realize their end users will not visit unless they trust in the protection of their private information. Using EV certificates provides the most reliable indicator of the trustworthiness of the site, and makes a very public statement of accountability to consumers.

Security industry solutions providers should work closely with CAs, which, as the survey shows, are important arbiters of online trust, with global standards that have been developed and refined over time. The security industry and CAs form a powerful duo that ensures retailers can earn consumers’ trust by enforcing the highest standards for identity vetting prior to issuing certificates. They can also serve as an effective educational resource for consumers and IT administrators to understand what SSL/TLS trust indicators mean.


3 “Extended Validation (EV) SSL Certificates: Improve Conversion Rates and Customer Confidence with Green Bar Assurance;” © 2003-2015 DigiCert® Inc • SSL Certificate Authority
https://www.digicert.com/ev-ssl-certification.htm
Who is the CA Security Council?

The CASC is comprised of leading global Certificate Authorities that are committed to the exploration and promotion of best practices that advance trusted SSL deployment and CA operations, and the security of the Internet in general.