Mess With A Horny Toad And You'll Get Messy

by Steve Brown

For those who grew up in AZ, you know a Horny Toad is not something to mess with. While not as risky as playing with its bigger cousin the Gila monster or a rattlesnake, these toads have their own predator protections built right in. When attacked, the Horny Toad squirts a stream of blood from the corners of their eyes that can launch up to 5 feet. In the ensuing chaos and confusion of the predator that has just been blasted, this wily critter scampers off into the desert.

Given the potential for a lawsuit, we obviously cannot recommend banks incorporate such defense mechanisms when it comes to cyber security. Instead, it makes more sense to move rapidly toward a future where methods like tokenization, biometrics and multifactor authentication will be the new normal to fend off attackers.

Let's start with tokenization and why it's so important. A token is nothing more than a reference that maps back to more sensitive data at the bank. In short, it replaces account information with a secure alternative. Unlike a personal account number, it is also useless if stolen. Here's how it works in simple terms. A person's card number is substituted by an alias number (token) that links back to the customer's real account through a highly secure server known as a vault. The token can be used the same way as a credit card number, but with this method, even if a retailer's system is comprised, thieves can only get the tokenized data.

A whole lot more is going on in the world of biometrics these days as well. In its simplest form, biometrics makes you the password. It includes fingerprints, eyes, voice, face, vein and signature patterns. This is important because Acuity research predicts biometrics will be used to authenticate 65% of all mobile commerce transactions in the next 5Ys. Today, research by Biometix finds usage of biometric technologies among banks by type is approximately: fingerprint (48%), finger vein (12%), voice (11%), hand vein (9%), iris (7%), signature (6%), hand geometry (5%) and face (3%). However, given the popularity of the smartphone, voice, face and finger are quickly jumping to the top of the list. The major bank leader in all of this is USAA who has already rolled out biometrics. They say customers love it and indicate finger and face take about 2 seconds to authenticate, while voice recognition takes about 20 seconds.

In terms of enhancing security, there is still room to improve but things are getting better. In fact, a recent Fed report found banks use the following methods to enhance security: multifactor authentication (84%); time out due to inactivity (78%); encryption (55%); mobile device ID (54%); mobile notifications (53%); out-of-band authentication (36%); geo-location (21%); tokenization (10%) and biometrics (6%).

Banks will always be targets of cybercriminals because that's where the money is of course. So, some ways to protect yourself include staying vigilant, using multifactor authentication, getting vulnerability assessments, protecting your data, shredding documents, having a data breach response program, rehearsing likely scenarios, having good insurance, having layered security and

preparing as much as you can. It is impossible to stop a country with limitless resources from hacking your little bank, but you can certainly try to manage and mitigate risk.

Predators will always sniff around trying to find prey, so in the cyber and security world it's up to your bank to continually evolve to protect yourself and your customers.

BANK NEWS

Branch Size

Codigo reports the current average branch size is 2,116 square feet.

Fintech

American Banker reports "Fintech" was the original name of a Citicorp project from the 1990s known as the Financial Services Technology Consortium. The term caught on and is now used widely (as "fintech") to mean anything digital related to financial technology ventures.

Cyber Partnerships

A survey by The Economist on cyber incident readiness by businesses finds companies indicate they have made arrangements with the following organizations as part of their incident response plans: IT forensic expert or other specialist IT provider (40%); specialist legal advisers (25%); police or other law enforcement (21%); communication provider (17%); insurance provider (16%); reputation management or crisis management firm (15%); PR or media agency (14%); and regulators beyond statutory requirements (11%). Of note, 23% said they did not have any arrangements in place.

Stock Investing

A survey by Natixis Global Asset Management finds 35% of Millennials think stocks will be the best-returning assets in 2016 vs. 46% for Gen X and 53% for Boomers.

Crisis Hangover

CNBC reports a study by Allianz Life finds 67% of Baby Boomers and Gen X say they still feel the effects of the financial crisis in their everyday lives.

Home Ownership

The percentage of households that own a home now sits at 63.4% as of Q2, the lowest level since 1967.

Branch Technology

Codigo reports the top branch technology institutions plan to include when remodeling branches are: digital signage (59%), tablet or kiosk (43%), overhead music (28%), interactive kiosk (28%), interactive tellers (27%) and video walls (13%).

Consumer Borrowing

CNBC reports new research by Card Hub finds the average indebted household's credit card balance has climbed to $7,813. This is the highest amount since 2008, when the average was $8,428.

Cloud

TheInfoPro projects worldwide cloud computing will grow at a 36% compound annual rate through next year, reaching a total market size of almost $20B.

Mobility

Research finds 90% of US adults now have a mobile phone.