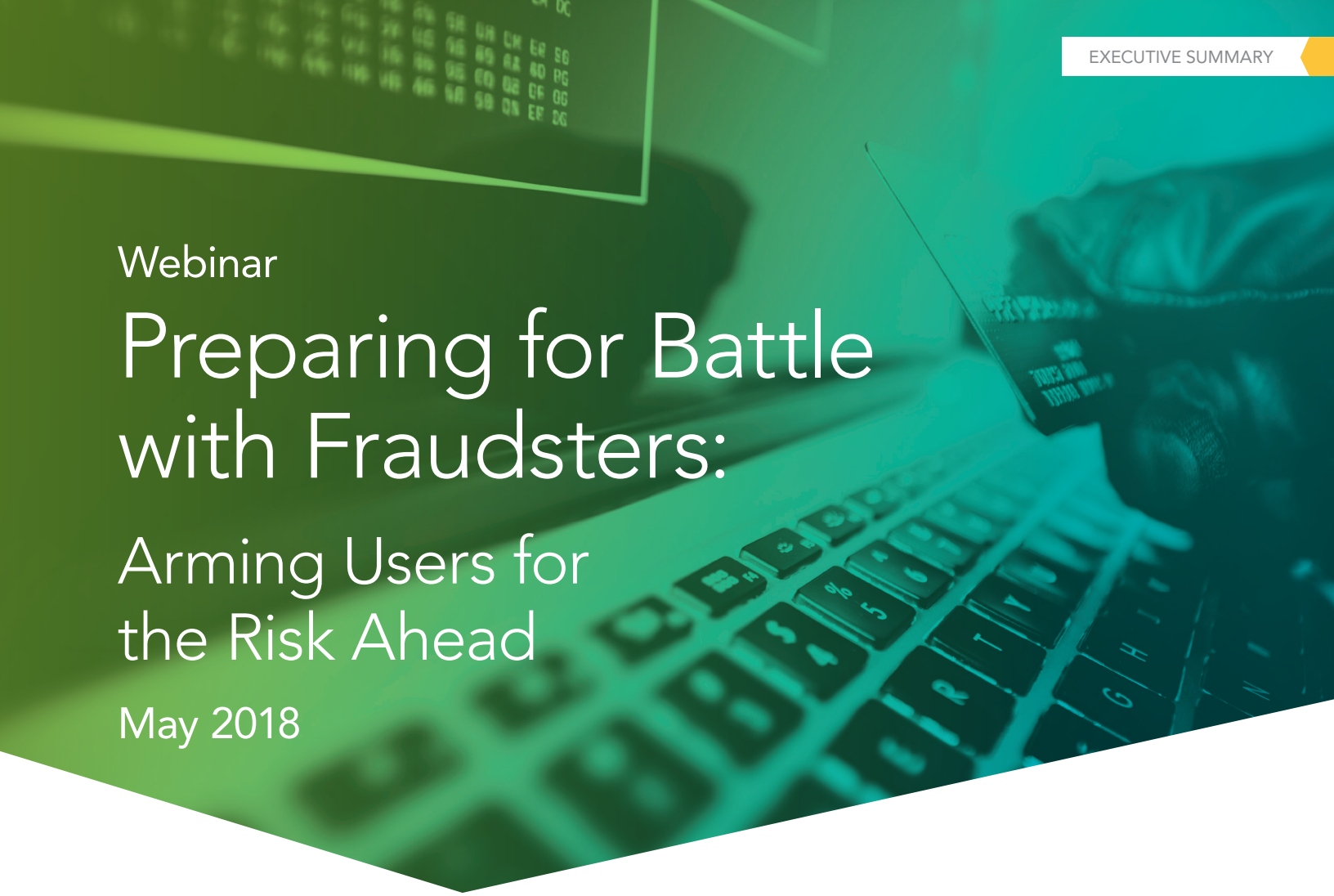

Webinar

Preparing for Battle with Fraudsters:

Arming Users for the Risk Ahead

May 2018

Most fraud isn't aimed at financial institutions, but rather their account holders. Arming account holders with the knowledge of common fraud scenarios and how to avoid them is critical to preventing fraud. Marketing and support teams should find creative ways to share these risks with account holders, so that they can actively protect themselves. Between your website and social media channels you've got a couple of different ways to evangelize the nature of threats and how best to avoid them.

Context

A proactive education campaign helps minimize exposure and losses related to fraud. It's important for account holders to be mindful of fraud methods, and for FIs to continue to teach vigilance against them.

Key Takeaways

Q2's Eric Jewell discusses different fraud scenarios and how they are typically carried out—and ways to combat fraudsters.

- Avoid or prevent fraud by making an impact on account holder behavior and by using different tools and services. Encourage account holders to report phishing emails to the FI.
- Remind account holders not to click on pop-ups or questionable ads. Only download materials from known and trusted sources and scrutinize attachments on email.
- Tell account holders that sensitive information shouldn't be shared with unvalidated individuals.
- Strongly encourage account holders to use a robust antivirus service on their computers. It's important that they have some level of protection to keep malware and viruses out.
- Suggest that account holders avoid using the same login and password on multiple sites. If an account holder has been affected, an organization should consider having another layer of defense in place, such as solid multi-factor authentication.
- A marketing or support team should consider creating a fun and entertaining way to help educate its account holders about fraud methods and how to prevent them—social media can provide a good option for sharing helpful information.

> "A great practice is simply encouraging account holders to log in regularly and stay on top of their balances and posted transactions, being aware of what's showing up in their account."

— Eric Jewell
Product Owner, Q2

Phishing

Phishing is one of the oldest existing scams. Fraudsters send emails that look and feel like they're originating from a victim's FI or any FI. Their goal might be to have an account holder enter their login credentials or other sensitive information or to go to a fraudulent website where they are exposed to malware. Smishing is a variant of phishing, in which a person receives a message via SMS/text message instead of email. In either case, the best defense is simply not clicking on the link. Teaching end users to be suspicious of inbound emails is important.

Vishing and Robocalls

Vishing and robocalls are equally troublesome. Sometimes fraudsters have some information about an intended victim but are missing some of key detail(s). A talented fraudster can typically pick up the phone and cleverly lead the victim to fill in the gaps. For example, some perpetrators claim they represent the Internal Revenue Service (IRS) to exploit people. They may call and ask a person to validate information or make a payment to cover a variance in their tax debt. In either case, they're looking for missing parts of the information puzzle. People should terminate the call if they believe it's not legitimate.

Malware

Malware is a broad topic and it comes in a lot of different forms—however, key loggers and ransomware are primary concerns. In today's social media world, people talk a lot about things going viral, and a primary risk of these infections is their ability to propagate and spread to other machines. Newer forms of malware can seize control of a machine and then spread through an organization's internal network ransoming or repurposing the machine for activities like mining crypto currency.

> "Users should always be directed to access the site from a commonly known URL. If you want to deliver a user a specific link directing them to somewhere on the page, like a special offer, send that information through a secure messaging service inside of your online banking."

— Eric Jewell
Product Owner, Q2

Fraud Account Grooming

Fraud Account Grooming is a strategy where the fraudster attempts to obfuscate their presence in the account by disabling alerts, redirecting out of band authentication, and changing contact information so that they fully assume the role of the legitimate user. In doing this they're able to withdraw larger amounts of money over a longer period of time, as opposed to an average criminal who is just looking for a quick score.

Other areas where fraudsters are active

Other areas where fraudsters are active include duping account holders and FIs through ACH and person-to-person payments—and increasingly through remote deposit capture.

> "There are a lot of different third-party places to get apps. We really do want to make sure that your users are staying close and pulling those apps only from the official Google and Apple stores, which have a formal review process."
>
> — Eric Jewell
> Product Owner, Q2

Other Insights

- Ideally, a third-party service can help combat and take down phishing sites. Q2 partners with Easy Solutions, whose Detect Monitoring Service works to quickly detect and shut down phishing sites.
- Anomaly detection systems can play an important role in preventing fraud. Q2 Sentinel, for instance, will suspend in real time those external transactions that do not follow the pattern of normal transactions.
- Behavioral analytics tools like Q2 Patrol can define when an account holder's login looks irregular and prompt the person to perform an out of band or step-up authentication prior to completing certain high-risk events.

Biography

Eric Jewell
Product Owner, Q2

Eric Jewell is a Product Strategist for Q2 security offerings. He has been active in the internet banking industry for 12 years. Prior to entering the industry, he was engaged in commercial lending for five years. He has an undergraduate and master's degree from the University of South Carolina.

For more information on Q2, go to Q2ebanking.com or call (512) 275-0072 ext. 2.