Safeguarding Network & Customer Credentials

Posted At : June 25, 2019 3:25 PM | Posted By : Admin
Related Categories: Security

This sotry is a bit long, kind of dense, but definitely worth the time to read. Years in the making, this FTC case shows how much damage a "bad actor" can cause to public facing networks.

Suppose a lunch companion says, “I think there’s something wrong with this tuna salad.” To determine if the problem is tuna not to their taste vs. tuna gone bad, would you scarf it down? Probably not. Now remove tuna salad from the example and substitute a web browser extension. (Stay with us here.) Let’s say you’ve been warned that an unknown extension could be used for fraud. Should you download it and let it marinate in your company’s network? **The FTC says that’s what the owner of ClixSense.com did**, and it’s just one example of conduct challenged as deceptive or unfair.

ClixSense – a sole proprietorship owned by James V. Grago, Jr. – is a rewards website that pays users for clicking on ads, taking online surveys, or completing other tasks. As part of the enrollment process, ClixSense collects users’ full names, addresses, dates of birth, and other personal information. In addition, people must create usernames and passwords and answer security questions. If users earn more than $600 a year from ClixSense, they have to turn over their Social Security numbers, too.

Visitors to ClixSense.com were promised “the latest encryption and security techniques to ensure the security of your account information.” But according to the **complaint**, at least through 2016, the site didn’t honor that claim. The FTC alleges that ClixSense didn’t perform network vulnerability and penetration testing, didn’t use established techniques to protect against third-party attacks, didn’t implement reasonable access controls, didn’t use techniques to detect cybersecurity events, and didn’t use encryption – among other techniques – to protect sensitive consumer information stored in plain text on its network.

What’s more, the FTC says ClixSense let employees store plain text user credentials in personal email accounts, didn’t change third-party default logins and passwords, failed to use readily available security measures, and maintained consumers’ information, including their Social Security numbers, in clear text on the company’s network and devices.

In November 2015, a user warned ClixSense about a publicly available browser extension that appeared to allow people to click on ads without actually viewing them. To use a term well-known in the industry, the browser extension purportedly facilitated click fraud. And that’s where the iffy tuna salad analogy comes into play, because how did ClixSense respond to the concern about this suspect browser extension? According to the FTC, ClixSense simply downloaded it onto its own network without taking proper precautions. There it sat for months as hackers used it to access credentials on employee laptops, change employees’ logins and passwords, and redirect visitors to an unaffiliated adult website – all clues that should have alerted ClixSense that its network had been compromised.

Ultimately, hackers used credentials lifted from an email on a compromised employee laptop to access an old ClixSense server still connected to the network. That server used the default credentials ClixSense had never changed. If lawsuits were horror movies, this is where you’d cover your eyes and yet still feel compelled to peek at what happened. That's because hackers used the old server to connect to the new server, which is where they downloaded personal information maintained in clear text on about 6.6 million consumers, 500,000 of them in the U.S. The hackers then offered stolen data for sale on a questionable website.

The complaint challenges the company’s claims about using “the latest security and encryption

techniques" as false or misleading. The FTC also alleges that the failure to use reasonable security was an unfair practice.

For people who follow FTC data security enforcement, the **proposed order** is worth a careful read. Among other things, the order prohibits misrepresentations about the privacy, security, confidentiality, or integrity of personal information, including the extent to which encryption and security techniques are used. In addition, before collecting personal information, Mr. Grago and any company he controls must put a comprehensive information security program in place. The proposed order lists eight specific features the program must have, all tied to the conduct and lapses alleged in the complaint. Also required: periodic third-party security assessments and annual certifications that the requirements of the order are in place. Once the proposed consent agreement is published in the Federal Register, you will have 30 days to file a public comment.

What can other companies take from this case?

Deliver on your security pledges. Security claims are more than cut-and-pasted boilerplate. Like any other objective representation, they need the support of solid substantiation.

Monitor for suspicious activity and respond quickly and thoughtfully. Use affordable tools to alert you to unexplained traffic on your network or changes to your website. If you suspect a security incident, implement a forceful red zone defense. But don't "investigate" with a wayward click or download your tech team hasn't thought through. Turn to the FTC's **Data Breach Response publication** and **video** for advice.

A confidential credential can be consequential. Most business people know that certain kinds of data – for example, Social Security numbers and account information – can be toxic to a consumer's identity if they fall into hackers' hands. But stolen login credentials can inflict harm, too. Let's face it: People have been known to use the same username and password on more than one site. Because the theft of a user's login on your site could serve as a skeleton key to give hackers access to consumers' bank accounts, medical records, or other highly sensitive information, keep a close eye on credentials. **Start with Security** has more tips on passwords and authentication.