Scams Heat Up During the Summer

Every day it seems there is a new scam warning, data breach notification, or privacy and security concern. It's almost impossible to keep up with them all. Each month, we take a look at some of the most recent scams, data breaches, and other issues and events that may put your personal information – and your identity – at risk. We also offer tips to help you protect yourself and avoid becoming a victim.

Privacy is Not Child's Play

CloudPets may not bite but they have been known to overshare. That's why they've been pulled from major retailers. Last year, the Bluetooth-enabled plush toys exposed data and children's voices; then email addresses and password information for more than 800,000 accounts were leaked.

Investigator Tip: ***When setting up any internet-connected device, provide the least amount required to activate the account. Consider using false information, including name, address, and date of birth. That way if the account is hacked, your actual information is not exposed.***

Do You Ever Get the Feeling Someone Is Watching You?

You may be right. Hackers are targeting webcams, security cameras and baby monitors that are controlled through the Yoosee mobile app. Once they have access, they can control cameras and watch a live stream. And it's not just strangers; exes are keeping eerily close tabs on former spouses and partners as a form of control. Some even consider it a form of domestic abuse.

Investigator Tip: ***Know how your internet-connected devices work and how to reset them. Always change the default password on any internet-connected device; also change it when someone moves out of the residence and anytime you think it may have been hacked.***

Traveling this Summer? Don't Get Burned!

You wouldn't hit the beach without sunscreen, so don't forget to pack your security sense when you hit the road. Whether you're traveling for business or pleasure, these tips can help you stay hacker-free.

Investigator Tip: ***Make sure you're doing everything you can to protect your information on the road, and at home. Call our Investigators at 888.494.8519 for more travel security tips and advice.***

Identity Thieves Driving up Fraudulent Auto Loans

What's an identity thief to do? "Chip" cards are making it harder for thieves to commit card fraud, so now they're turning to auto loans, building a credit history by combining legitimate PII with fake info to create a "synthetic" identity.

Investigator Tip: ***IDShield members receive an alert when new credit activity is detected, along with unlimited consultation. If you receive an alert for activity you don't recognize, call our Investigators who can discover if it is a simple error or cause for concern.***

Hello. This Is a Robocall.

More than 4 billion robocalls were placed in June. Chances are, you got a few of them yourself, even if you're on the Do Not Call registry. Almost all of these calls are scams that sound just legitimate – or scary – enough to take a victim's money.

Investigator Tip: ***Robocalls, with the exception of those from political candidates, are illegal from companies you haven't given written permission to call you. Visit myidshield.com and learn how you can sign up for the Do Not Call registry on our newly updated "Reduce Mail and Phone Solicitation" page. Be advised that the companies making illegal robocalls do not reference this registry. Don't answer calls from numbers you don't recognize.***

Scammers at Work

Jobseekers: beware. The "work from home" scam promises high incomes for those who buy into their "system." Turns out, the only ones making a lot of money are the scammers, who may be getting jobseekers' information from job listing and recruitment portals. Scammers may also access a legitimate business account to post phony jobs.

Investigator Tip: ***If it sounds too good to be true, it probably is. Be suspicious of any unsolicited job offers or "business opportunities" that you receive through email. Verify job postings by calling the company or visiting their website to see if they are hiring for the posted position.***

JUNE DATA BREACHES

Breached Entity	Information Exposed	# of Consumers Affected
PDQ Restaurants	Payment card information including account numbers, names and expiration dates	Unconfirmed
Adidas	Customer contact details, physical addresses, and email information; possibly login information (usernames and encrypted passwords.	Unconfirmed
Exactis	Non-financial data including phone numbers, addresses, emails, habits, number of children, etc.	Nearly 340 million
MyHeritage	Email addresses and hashed passwords	>92 million

Remember, as an IDShield member you have unlimited consultation with Kroll's Licensed Private Investigators. If you have a question about a scam, have received a suspicious email, or received a breach notification, give us a call at 888.494.8519. We're available to answer your questions Monday-Friday, 7 a.m. – 7 p.m. CT.