

Office of Research Security Newsletter

December 2019

Avoid Holiday Shopping Scams

Don't Fall Victim to Online Schemes

Tis the season for holiday gifting, and many shoppers will go online this time of year to find the best deals on popular items. But the sellers you buy from may not be what they seem.

According to the FBI's [Internet Crime Complaint Center \(IC3\)](#), thousands of people become victims of holiday scams every year. Scammers can rob you of hard-earned money, personal information, and, at the very least, a festive mood. The two most prevalent of these holiday scams are non-delivery and non-payment crimes.

In a non-delivery scam, a buyer pays for goods or services they find online, but those items are never received. Conversely, a non-payment scam involves goods or services being shipped, but the seller is never paid. In 2018 alone, the IC3 estimates that non-delivery and non-payment scams together affected more than 65,000 victims, causing almost \$184 million in losses.

Similar scams to beware of this time of year are auction fraud, where a product is misrepresented on an auction site, and gift card fraud, when a seller asks you to pay with a pre-paid card.

To Read the Full Article - <https://www.fbi.gov/news/stories/avoid-holiday-shopping-scams-112719>



*Office of
Research
Security would
like to wish you
a happy and
safe holiday
season! We are
looking forward
to seeing you
back in 2020!*





Understanding the Ripple Effect: Large Enterprise Data Breaches Threaten Everyone

Tara Seals / November 8, 2019

Fallout from giants at the top is one of the largest drivers of cyber-impacts on everyday people and companies.

Big businesses are constantly under attack, and that affects everyone from customers and business partners to parties with national security interests.

When successful, the initial compromise is only a means to an end — the real goal is to mount follow-on attacks like spearphishing, extortion attempts and account takeover (ATO). And much to the more than 6,500 data breaches, exposing a staggering 5 billion compromised records, according to Risk Based Security.

“Breaches against large enterprises are becoming more frequent. There are several reasons for this – notably, breaches are no longer standalone incidents, they are part of larger organized cybercrime networks,” said Arun Kothanath, chief security strategist at Clango, in an interview.

The second reason, Kothanath said, was that the price of data is skyrocketing: Beyond data tied to financial institutions being an attractive target, so is data tied to healthcare, education, infrastructure, elections and national security.

To read the full article –

https://threatpost.com/ripple-effect-large-enterprise-data-breaches/150041/?utm_source=360Works%20CloudMail&utm_medium=email&utm_campaign=NewsWatch



We will be out and about visiting your department soon...



The Science Security Threat

By: Doug Lederman | November 13, 2019



At gathering of university research officers, federal agency officials document foreign governments’ efforts to persuade scientists to engage in academic espionage.

SAN DIEGO – Some of the university research administrators in the audience seemed loaded for bear, ready to scold the Trump administration officials in front of them for what many academics have perceived to be radical profiling of Chinese scientists in recent months.

Roger Wakimoto, vice president for research at the University of California, Los Angeles, didn’t soft-pedal the issue as he introduced the session on science and security here Monday at the annual meeting of the Association of Public and Land-grant Universities.

“We’ve been told repeatedly that this is a partnership,” Wakimoto said of the effort to “protect U.S. science from undue foreign influence,” as the session was titled. “If this is a partnership, stopping our faculty at the airport is not acceptable.”

To read the full article –

<https://www.insidehighered.com/news/2019/11/13/federal-officials-document-international-threats-us-science-security>



OFFICE OF RESEARCH SECURITY STAFF

DENISE SPILLER
SECURITY ADMINISTRATOR
824-6444 / denise.spiller@uah.edu

CAITLYN SCHOENIG
SECURITY ASSISTANT
824-4717/cns0017@uah.edu

JANINE WILSON
ASSOCIATE SECURITY ADMINISTRATOR
824-3025 / janine.wilson@uah.edu

MARIAH WILKINSON
STUDENT SPECIALIST II
824-4818/mw0077@uah.edu

APRIL MCMEANS
ASSISTANT SECURITY ADMINISTRATOR
824-6048 / april.mcmeans@uah.edu

RYAN WILKINSON
STUDENT SPECIALIST I
824-4818/ryan.wilkinson@uah.edu