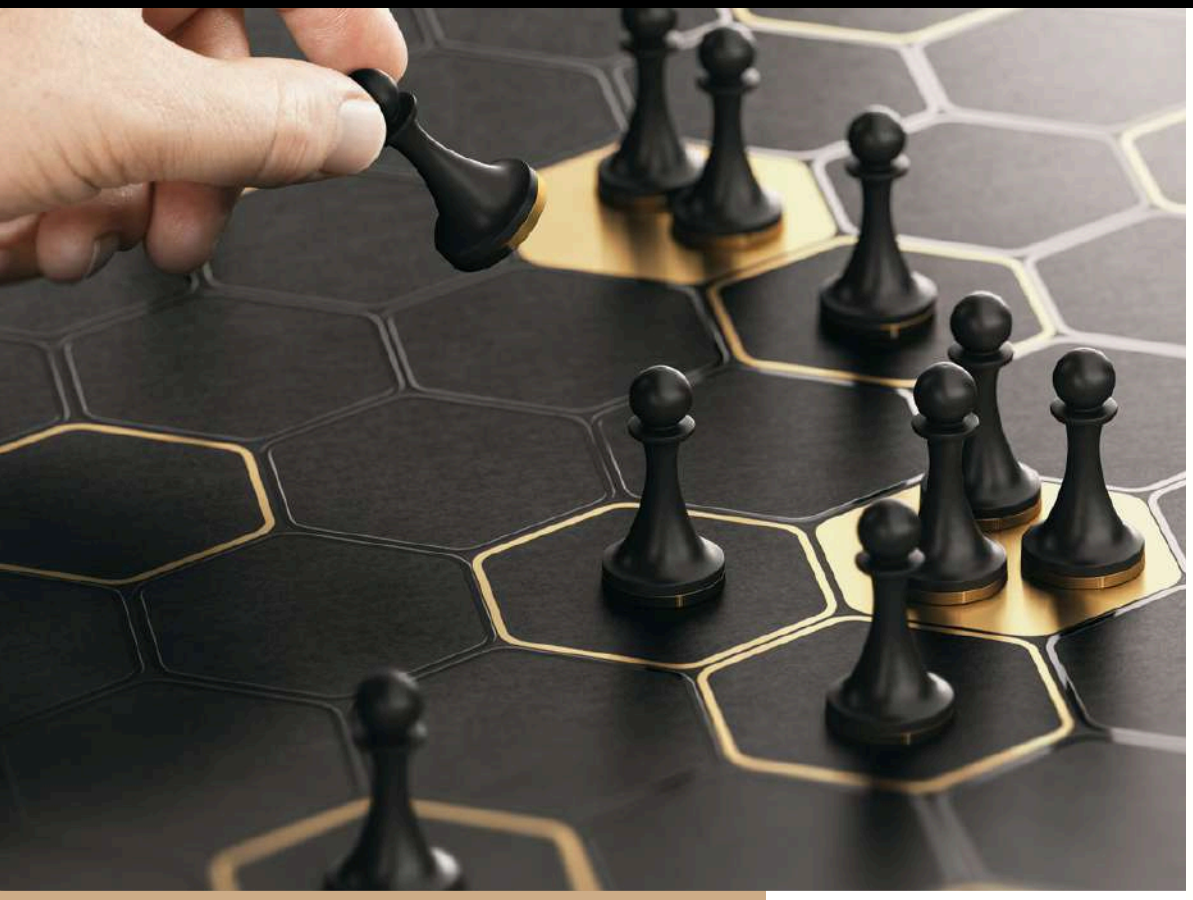
RECOGNIZING SCAM STRATEGIES

Tackling the complexities of BEC and real estate scams



THIS MONTH'S TOPICS:

Real Estate Scams

The property scams circulating the web

BEC Scam Strategies

The multi-step strategies of scammers

Scam of the Month:

Utility Company Scams...

Monthly Cyber News:

News and Upcoming Holidays...

From deceptive emails to sophisticated social engineering ploys, cybercriminals are using complex strategies to carry out their scams. Luckily, there are many things we can do to stay a step ahead of our opponents in the world of cybersecurity.

In this month's newsletter, we dive into the increasingly complex world of BEC scams, unveiling the latest strategies that cybercriminals are using to target individuals and organizations. We also take a close look at real estate scams—a pressing concern for anyone looking to rent or buy a property.

REAL ESTATE SCAMS

Real estate scams are increasingly targeting homebuyers, sellers, and renters, resulting in significant financial losses. Below are four common real estate scams and protective measures to avoid them.

DECEPTIVE WIRE TRANSFERS

- How it works: Scammers use timely BEC attacks to intercept wire transfers related to property purchases. They pretend to be one party (either the buyer, the lawyer, or the mortgage issuer, depending on who they are targeting) and provide their account details for the money to be wired to.
- Protection: Use secure communication, verify payment instructions via trusted channels, and verify details in person when possible. If you receive a message from a scammer posing as a lawyer or mortgage issuer, report it and alert the person being impersonated.

RENTAL LISTING SCAMS

How it works: Fake rental listings posted at cheap prices lure users into sending money to secure the rental before seeing it.

Protection: Verify property details, avoid unsecured payments, and inspect properties in person.

DEED & TITLE FRAUD

How it works: Fraudsters transfer property ownership without consent by stealing the owner's identity or using a phony title to sell the property to someone else.

Protection: Regularly monitor property titles, consider title insurance, and secure personal information.

MORTGAGE AND FORECLOSURE RELIEF

How it works: Scammers promise relief services for small fees but don't deliver.

Protection: Research the organization, use legitimate sources, avoid upfront payments, and report suspicious activities.

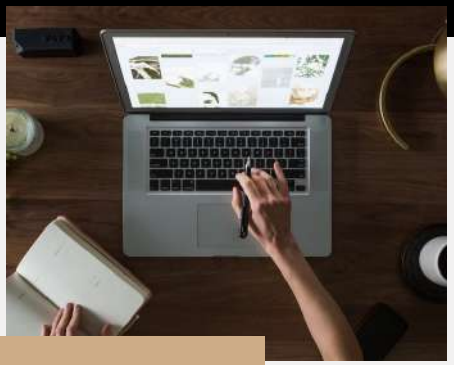
BEC SCAM STRATEGIES

Scammers are using complex strategies to craft multi-step Business Email Compromise scams.

What are BEC Scams?

Business Email Compromise (BEC) scams are a sophisticated type of cybercrime where attackers pose as trusted members within an organization or a known third-party to trick employees into transferring money or giving them access to sensitive information.

Unlike typical phishing attacks, BEC scams usually target specific individuals.



In a specific type of BEC scam that is circulating, scammers send a message with a fake email chain below it that appears to show a history of correspondence between the user and an employee of a familiar third-party company. The scammer mimics the company's email template, complete with logos and disclaimers.

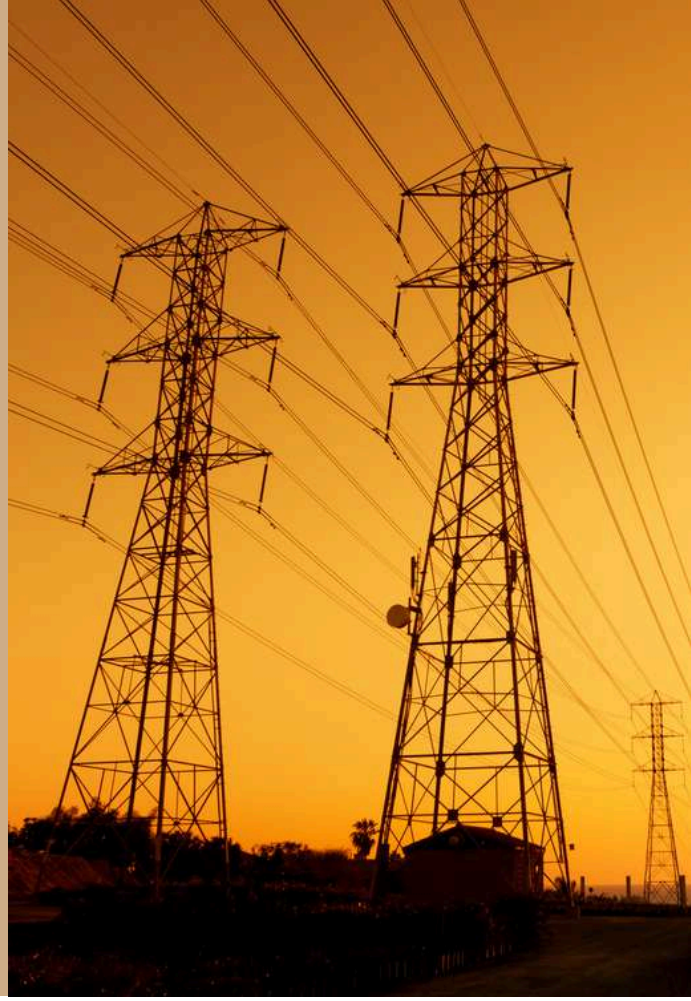
The email might include details that are surprisingly specific, such as a recent purchase or subscription. The fraudster may introduce themselves as a member of a department like customer service.

Beat the competition:

- In these scams, the cybercriminal often brings up an urgent matter such as a billing discrepancy, or a security alert to get you to click a malicious link or hand over financial information.
- Verify the sender's email address and reach out to a known or official contact at the company in question.

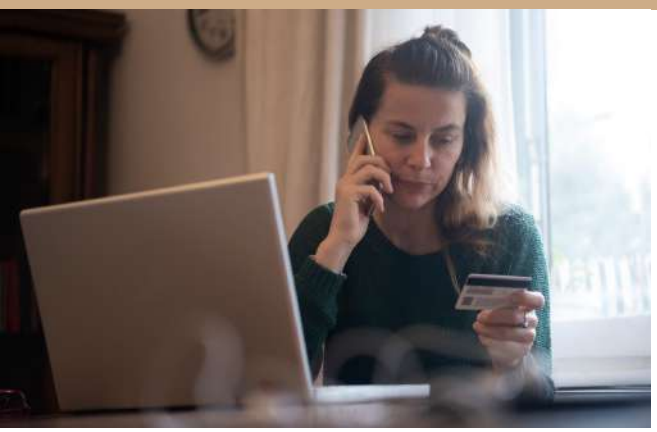
SCAM OF THE MONTH

Each month we highlight a scam that demonstrates tactics criminals are using RIGHT NOW, to better prepare you when the next scam hits.



Sarah had always been cautious with her finances, but one scorching summer day, her phone buzzed with an urgent call. "This is your electric company. Your bill is overdue, and your power will be shut off in an hour if you don't pay $250 immediately via a prepaid debit card." Panic set in as she imagined her kids sweltering in the heat. She frantically checked her email and mailbox for missed bills but found nothing. Her anxiety grew as the caller's urgency intensified.

Without thinking, she rushed to the nearest store, bought a prepaid debit card as instructed, and called back the number. The voice on the other end guided her through the payment process, ensuring she provided all the necessary details. It wasn't until the stress of the phone call wore off that she realized she should have verified the caller's legitimacy. Sarah looked up her electric company's real phone number and called. The electric company confirmed her fear—it was a scam. They had no record of such a call or payment.



Did you spot the red flags?

- The scammer used high-pressure tactics, creating a sense of urgency.
- Sarah was instructed to pay via a prepaid debit card, a common red flag in scams.
- Sarah should have hung up and called the legitimate customer service number to verify the claim.

Legitimate utility companies accept various payment methods and don't pressure customers to pay immediately via wire transfer or prepaid debit card under threat.

If someone shows up at your home unannounced, claiming to be from a utility company and demanding immediate payment, it is likely a scam. Do not let these unsolicited visitors into your home unless you have made an appointment or reported an issue.

CYBER NEWS

AUGUST
2024

DATA BREACH LEADS TO SCAMS

Scammers are capitalizing on a recent data breach by making websites claiming to check if a user's social security number was impacted. When a user enters their information on one of these fake websites, their data goes to the scammer. While there are some legit websites that check if your data has been leaked, it is best to avoid entering your social security number into random websites. Instead, check your credit reports for unexpected activity. Reach out to the major credit bureaus and notify them if you notice any suspicious activity.

UPCOMING HOLIDAYS

September 9th is Sudoku Day. Like cybersecurity, sudoku involves problem-solving and analysis. Just like sudoku, users should take their time analyzing the details of a potential scam before acting.

FAKE INVOICE IMPOSTER SCAMS

Cybercriminals are adding fake invoices to emails. The fake invoice urges the user to call the number provided to dispute the charge made on their account. The scammer then claims they accidentally sent too much money for the refund and asks the user to send the larger amount back to them in Bitcoin. Use caution with unsolicited emails about account issues. Go directly to the account or look up the company's customer service number instead.