FRAUD PREVENTION FRIDAY

Friday, August 23, 2024

Top News

- Want To Learn How To Steal A Password? It's Easier Than You Think
- The AI Battle: Cybercriminals Vs. Fraud Prevention Experts
- Cybersecurity Awareness Month Resource Kit User Guide
- Understanding Cyber Threats
- New Phishing Attack Uses Sophisticated Infostealer Malware

Want To Learn How To Steal A Password? It's Easier Than You Think

Passwords are one of the most important parts of keeping any account secure, and if you were to gain access to these accounts, you'd have access to personal data, subscriptions, money, and even the victim's identity. CBM Associate Member RedRock Information Security wants to show you just how easy it is to steal a password and gain access to an account.

All it takes is a little spare cash to gain access to any account, and it's remarkably easy to pull off. We can't show you exactly how to do it, but we want to emphasize that literally, anyone can do this to your business. Let's look into some of the intricacies of how stealing a password works.

We'll use Homer J. Simpson for our example, a name with a singular entry in the United States census from 1940. Simpson was born in 1914, and we are confident that there have not been any babies born with the name since the 90s. That said, we're making everything up from here on out. If we want to make Simpson's life difficult, it's pretty easy to do so, even if we don't know anything about him.

(Click the link above to continue reading)

The AI Battle: Cybercriminals Vs. Fraud Prevention Experts

The current landscape in today's fraud prevention requires artificial intelligence (AI) and machine learning for a more proactive approach to safeguarding the financial industry from bad actors. However, criminals are finding new and improved ways to use AI to commit fraud. The financial sector is a prime target for cybercriminals, so banks, financial institutions and payment transaction providers constantly look for ways to improve their defensive strategies for the sake of their customers and their bottom line.

In March 2024, the U.S. Treasury Department reported that the banking industry is finding it hard to keep one step ahead of fraudsters who are using AI to pretend to be customers and spread malware using AI-generated content. In fact, last year these fraudsters cost Americans a total of $12.5 billion. Huron Consulting, which works with banks and financial institutions, predicted last June that about 50% of these organizations have or will adopt AI as a defensive action to combat this increasing fraud.

Fraud prevention has needed to become stronger, smarter and faster for good reasons. Fraudsters find sneaky ways to use AI to steal from banks and financial institutions. Synthetic identity theft is on the rise where AI can be used to generate realistic fake identities, complete with social media profiles. This type of fraud even manages complete account takeovers where AI has automated processes for finding and compromising real user accounts by cracking passwords or exploiting vulnerabilities with multifactor authentication. As such, fraudulent accounts have been opened and security checks bypassed.

(Click on the link above to continue reading.)

Cybersecurity Awareness Month Resource Kit User Guide

October is known as Cybersecurity Awareness Month, a time to emphasize the importance of securing our digital lives and fostering best practices in online safety. This annual event, spearheaded by cybersecurity advocates, aims to educate individuals and organizations on how to protect their networks, data, and personal information from the increasing threat of cyber attacks. It encourages a proactive stance towards cybersecurity, equipping everyone with the knowledge to recognize potential threats and adopt preventive measures.

A vital resource for organizations during this month is the Cybersecurity Awareness Month Resource Kit User Guide by KnowBe4. This guide offers a comprehensive toolkit designed to help organizations strengthen their cybersecurity culture. With actionable insights, phishing simulation ideas, and awareness materials, the guide empowers companies to engage employees in cyber safety practices throughout the month and beyond. KnowBe4's resource is particularly valuable in helping IT departments and leaders build a more resilient defense against cyber threats through education and awareness initiatives.

This October, leverage these resources to fortify your organization's defenses and cultivate a secure cyber environment for all.

Understanding Cyber Threats

The one thing cybersecurity threats have in common is that they are harmful and the cybercriminal is committed to destroying, stealing, or disrupting data, critical systems, and digital life in general. Your financial institution uses numerous security applications and incorporates processes to keep your financial information and assets secure and to comply with regulatory guidelines.

However, security is everyone's responsibility, and you can do the following three things to help safeguard your assets.

First, educate yourself about the various tactics, techniques, and processes (TTP) cybercriminals use to steal from you. TTPs are like fashion – what's in style one month is out-of-date the next – so cybercrimes change over time.

Second, install security applications on your personal computers and mobile devices. Those applications – especially anti-virus and content-blocking applications – are an additional layer of protection for devices connected to the outside world. It's important to secure all your devices, especially those used by your whole family.

As tempting as free security applications are, they aren't always the best way to protect your financial data. Research and select applications offering the best protection. Consider it an investment that protects you from the hassles of restoring your online financial life to some degree of normal.

(Click the link above to continue reading.)

New Phishing Attack Uses Sophisticated Infostealer Malware

A new sophisticated phishing attack featuring a stealthy infostealer malware that exfiltrates a wide range of sensitive data has been uncovered by threat analysts.

This malware not only targets traditional data types like saved passwords but also includes session cookies, credit card information, Bitcoin-related extensions and browsing history.

The collected data is then sent as a zipped attachment to a remote email account, highlighting a significant shift in infostealer capabilities.

According to an advisory published by Barracuda Networks, the attack begins with a phishing email that entices recipients to open an attached purchase order file.

These emails, characterized by grammatical errors, appear from a fake address. The attachment contains an ISO disc image file, a precise replica of data from optical discs like CDs or DVDs. Embedded within this image file is an HTA (HTML Application) file, which enables the execution of applications on the desktop without the security limitations of a browser.

(Click the link above to continue reading.)