

# Inspired eLearning May Newsletter



## **Blog: How to Protect Your Organization from CEO Fraud**

CEO fraud is a cyber attack strategy that costs businesses millions of dollars. Learn how to handle CEO fraud and avoid these costly mistakes.

[READ BLOG](#)



## **Blog: HIPAA Security Rule and Compliance Checklist**

HIPAA compliance is a necessity for any organization in the healthcare industry. This HIPAA security rule checklist has the need to know information.

[READ BLOG](#)

## **FBI Says Cybercrime Complaints More Than Doubled In 14 Months**

The FBI's Internet Crime Complaint Center (IC3) has seen a massive 100% in cybercrime complaints over the past 14 months.

When the IC3 first began logging complaints in 2000, it took seven years to reach 1 million complaints. Since then, it has taken an average of 29.5 months for each additional million complaints.



For the period between March 2020 and May 2021, the IC3 saw a massive increase of 1 million complaints in just 14 months.

The FBI attributes the rise in complaints to cyber criminals taking advantage of people working from home due to the pandemic and the rise in COVID-19 themed attacks.

"In 2020, while the American public was focused on protecting our families from a global pandemic and helping others in need, cyber criminals took advantage of an opportunity to profit from our dependence on technology to go on an Internet crime spree," says the IC3's 2020 Internet Crime Report.

"These criminals used phishing, spoofing, extortion, and various types of Internet-enabled fraud to target the most vulnerable in our society - medical workers searching for personal protective equipment, families looking for information about stimulus checks to help pay bills, and many others.

As part of the report, the FBI says the top three crimes reported in 2020 were phishing scams, non-payment/non-delivery scams, and extortion.

However, victims lost the most money to BEC scams (\$1.8 billion in losses), romance scams (\$600 million in losses), and investment fraud (\$336 million).

This article was originally posted by Bleeping Computer. Read the full article [here](#).

---

### **Fake Android, iOS Apps Promise Lucrative Investments While Stealing Your Money**

*Hundreds of malicious cryptocurrency, stock, and banking apps have been discovered by researchers.*

Researchers have discovered hundreds of malicious mobile apps that are exploiting interest in cryptocurrency and stocks to steal from victims.

Sophos researchers said on Wednesday that a tip-off relating to a fake mobile trading app led to the discovery of a server containing "hundreds" of malicious trading, banking, foreign exchange, and cryptocurrency apps designed for the Android and iOS platforms.



Mobility has meant that stock trading and investment opportunities are now widely available and far more accessible than before. Rather than having your money managed by a particular fund or agency in return for a fee, users can now select their own investments with a single swipe.

Social media has become a hotbed of pump-and-dump or "meme" stock chat and trading tips, and cryptocurrency, too, has become a popular topic of discussion for eager investors.

However, the ease of downloading a mobile application to explore investment opportunities has also created an avenue for cybercriminals to exploit.

According to Sophos, the apps found included counterfeit software created to impersonate well-known, legitimate, and trusted brands including Barclays, Gemini, Kraken, TDBank, and Binance.

The operators have created dedicated websites linked to each individual app, tailored to appear as the impersonated organizations in an effort to improve the apparent legitimacy of the software -- and the likelihood of a scam being successful.

Sophos' investigation into the apps began with a report of a single malicious app masquerading as a trading company based in Asia, Goldenway Group.

The victim, in this case, was targeted through social media and a dating website and lured to download the fake app.

Rather than relying on mass spam emails or phishing, attackers may now also take a more personal approach and try to forge a relationship with their victim, such as by pretending to be a friend or a potential love match. Once trust is established, they will then offer some form of time-sensitive financial opportunity and may also promise guaranteed returns and excellent profits.

However, once a victim downloads a malicious app or visits a fake website and provides their details, they are lured into opening an account or cryptocurrency wallet and transferring funds. Scammers will then vanish with the money and block their victims.

Sophos says that the apps discovered on the server were being pushed through the same infrastructure and through a "Super Signature process" abused to bypass security protections and mechanisms used by official app repositories.

In the case of iOS, the process -- designed for small app developers to conduct legitimate test deployments before submission -- requires a target device to download and install a manifest file to accept the package, and then the device's ID is sent to a registered developer account. An .IPA package containing the app is then pushed to the user for download.

"While many of these Super Signature developer services may be targeted at helping legitimate small app developers, we found in our investigation that the malware used many such third-party commercial app distribution services," the researchers say. "These services offered options for 'One-click upload of App Installation' where you just need to provide the IPA file. They advertise themselves as an alternative to the iOS App Store, handling app distribution and registration of devices."

In some cases, the distribution services dropped web clips that added a link to a malicious web page directly to a victim's home screen rather than pushed IPA files.

When it comes to Android abuse, users are asked to install and launch an app, create an account,

and then begin trading. The apps appeared to be real and in some cases included elements such as cryptocurrency price tracking. However, wallets are either controlled by cybercriminals or the funds required to start trading are requested to be sent to bank accounts registered in Hong Kong.

It appears that Asia is primarily being targeted by the network, as one of the servers referenced in an app led to the discovery of uploaded records including ID cards, driver's licenses, passport photos, and more from nationals in South Korea, China, Malaysia, and Japan.

"We believe the ID details could have been used to legitimize financial transactions and receipts by the crooks as a confirmation about the deposits from the victims," Sophos says. "We also found several profile pictures of attractive people likely used for creating fake dating profiles, which suggests that dating could have been used as a bait to lure victims."

For more details, read the full article [here](#).

---

### **Magecart Hackers Now hide PHP-Based Backdoor In Website Favicons**

Cybercrime groups are distributing malicious PHP web shells disguised as a favicon to maintain remote access to the compromised servers and inject JavaScript skimmers into online shopping platforms with an aim to steal financial information from their users.



"These web shells known as Smilodon or Megalodon are used to dynamically load JavaScript skimming code via server-side requests into online stores," Malwarebytes Jérôme Segura said in a Thursday write-up. "This technique is interesting as most client-side security tools will not be able to detect or block the skimmer."

Injecting web skimmers on e-commerce websites to steal credit card details is a tried-and-tested modus operandi of Magecart, a consortium of different hacker groups who target online shopping cart systems. Also known as formjacking attacks, the skimmers take the form of JavaScript code that the operators stealthily insert into an e-commerce website, often on payment pages, with an intent to capture customers' card details in real-time and transmit them to a remote server.

While injecting skimmers typically work by making a client-side request to an external JavaScript resource hosted on an attacker-controlled domain when a customer visits the online store in question, the latest attack is a little different in that the skimmer code is introduced into the merchant site dynamically at the server-side.

The PHP-based web shell malware passes off as a favicon ("Magento.png"), with the malware inserted into compromised sites by tampering with the shortcut icon tags in HTML code to point to

the fake PNG image file. This web shell, in turn, is configured to retrieve the next-stage payload from an external host, a credit card skimmer that shares similarities with another variant used in Cardbleed attacks last September, suggesting the threat actors modified their toolset following public disclosure.

Malwarebytes attributed the latest campaign to Magecart Group 12 based on overlaps in tactics, techniques, and procedures employed, adding "the newest domain name we found (zolo[.]pw) happens to be hosted on the same IP address (217.12.204[.]185) as recaptcha-in[.]pw and google-statik[.]pw, domains previously associated with Magecart Group 12."

Operating with the primary intention of capturing and exfiltrating payment data, Magecart actors have embraced a wide range of attack vectors over the past several months to stay under the radar, avoid detection, and plunder data. From hiding card stealer code inside image metadata and carrying out IDN homograph attacks to plant web skimmers concealed within a website's favicon file to using Google Analytics and Telegram as an exfiltration channel, the cybercrime syndicate has intensified in its efforts to compromise online stores.

Skimming has become so prevalent and lucrative a practice that the Lazarus Group, a collective of state-sponsored hackers affiliated with North Korea, attacked websites that accept cryptocurrency payments with malicious JavaScript sniffers to steal bitcoins and ether in a new campaign called "BTC Changer" that started early last year.

This article was originally posted on The Hacker News. Read the full article [here](#).

---

## Product Updates

We have exciting new updates to share! Click below to learn more about what Inspired eLearning is doing to better our product experience for our customers.

LEARN MORE

Connect with us:



© 2021 Inspired eLearning, LLC. All rights reserved.

info@inspiredelearning.com | 800.631.2078

4630 N Loop 1604 W, Suite 401

San Antonio, TX 78249 USA

[Privacy Notice](#)