Vol. 11 | Issue 6

NEWS CYBER SECURITY

June 2026

| Page 2 | Page 3 | Challenge |

Welcome to the TXDPS Cyber Security Newsletter

One big thing: World Cup Fever Means More Scams

What to know: The 2026 FIFA World Cup kicks off June 11 – and cybercriminals are already taking advantage of the hype. They love major global events because people let their guard down.

Security researchers and consumer watchdogs are warning about a surge in World Cup-themed scams, phishing emails, fake ticket offers, bogus travel sites, and dangerous streaming links targeting excited fans.

What to watch for:

- **Fake ticket sites** offering "exclusive access," deep discounts, or resale tickets that never arrive.
- **Fraudulent travel booking pages** impersonating airlines, hotels, or event packages.
- **"Free streaming" links** that lead to malware, fake login pages, or sketchy browser downloads.
- **Phishing emails and texts** pretending to be FIFA, sponsors, or ticketing platforms asking you to "verify" accounts or payment info.

Stay safe:

- Buy tickets only through official or trusted sources.
- Avoid links from social media comments or unsolicited emails.
- Don't install "special video players" to watch matches.
- Double-check URLs before entering passwords or payment info.
- Use credit cards when purchasing/traveling for added fraud protection.

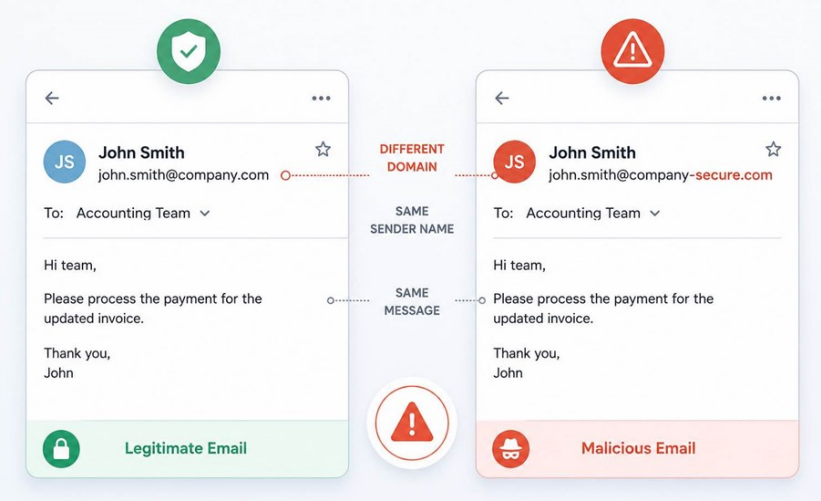
More on these scams: https://www.malwarebytes.com/blog/threat-intel/2026/05/the-2026-world-cup-scam-economy-is-already-running-before-the-first-whistle

Business Email Compromise

Most phishing emails try to grab your attention.

Business Email Compromise (BEC) goes a step further – it tries to earn your trust.

BEC attacks happen when a cybercriminal impersonates a trusted person or organization to convince someone to send money, share sensitive information, or take urgent action. These messages often appear to come from executives, coworkers, vendors, or business partners.



So...is BEC the same as phishing?

BEC is a *form* of phishing, but it's usually more targeted and convincing.

Traditional phishing often relies on suspicious links or attachments. BEC attacks may contain neither. Instead, attackers use impersonation, urgency, and believable business scenarios to trick people into acting quickly.

Common examples include:

- A "CEO" requesting a wire transfer.
- A vendor sending "updated" payment instructions.
- A coworker asking for gift cards or payroll information.

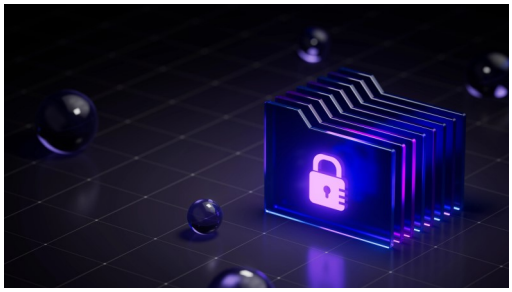
BEC remains one of the most financially damaging forms of cybercrime because it targets human trust more than technology.

How to stay safe:

- **Slow down with urgent requests.** Attackers rely on pressure and urgency.
- **Verify payment or banking changes.** Use a known phone number or trusted contact.
- **Check sender details carefully.** Small spelling or domain changes matter.
- **Be cautious with unusual requests from leadership.** Especially requests involving money or sensitive data.
- **When in doubt, ask.** A quick verification can prevent a costly mistake.

In the News

FBI warns about fast-growing phishing kit targeting Microsoft 365 users



(Matt Kapko | May 22, 2026)

"The FBI is warning organizations and defenders about Kali365, a growing phishing-as-a-service platform that retrieves Microsoft 365 access tokens, issuing a public service announcement Thursday.

The toolkit bypasses multi-factor authentication and abuses OAuth device code authorizations via phishing lures impersonating common enterprise services. This technique grants cybercriminal-controlled applications access to Microsoft 365 accounts, opening victims up to a host of follow-on malicious activity, including data theft, fraud, extortion and ransomware attacks.

Kali365 is one of many rapidly emerging device-code phishing tools, which are gaining popularity as a more effective means for cybercriminals to circumvent security controls while abusing legitimate Microsoft device authorization pages, according to researchers.

Instead of gaining access to accounts via phishing kits that steal credentials and second-factor authentication codes, device-code phishing platforms connect a malicious app to a legitimate account with a single code. The process requires fewer steps and less interaction with the user, but victims do have to copy-and-paste a code generated by the Kali365 platform to grant access.

'We see quite a bit of this device-code phishing activity, but so much of it looks really similar. They're all using the same types of lures, the same types of content, the same branding,' Selena Larson, senior threat researcher at Proofpoint, told CyberScoop. 'It is very much AI generated, AI driven, and the threat actors, I think, are finding it pretty effective because we're seeing this shift happen kind of all at once.'"

Full Story: https://cyberscoop.com/fbi-phishing-kali365-microsoft365-access-tokens

A Few More Cyber News Stories:

Report: Deepfake Fraud Causes Billions in Losses
https://blog.knowbe4.com/report-deepfake-fraud-causes-billions-in-losses

Anthropic: Mythos finds more than 10,000 software flaws in first month
https://cyberscoop.com/anthropic-mythos-software-flaws-glasswing

FBI: Hackers Sending Operatives in Person to Insert USB Drives and Steal Data
https://www.securityweek.com/fbi-hackers-sending-operatives-in-person-to-insert-usb-drives-and-steal-data

CYBER CHALLENGE

Phishing Websites

This Month's Challenge

For this month's challenge, let's see how well you do spotting a fake website trying to steal your login credentials.

There are 14 of these to look at and decide if they are real or a phishing site.

Let me know how you do! Good luck.

https://www.opendns.com/phishing-quiz