Country Club Bank Member FDIC
epcor Electronic Payments Core of Knowledge
PAYMENTS INSIDER
The inside scoop on payments for businesses of all sizes

Navigating the Treacherous Waters of Election Phishing Scams

In an age where information is as accessible as air, the upcoming election season has become fertile ground for fraudsters to sow seeds of deceit and misinformation. As the political atmosphere thickens with anticipation, voters find themselves bombarded with a myriad of messages, each competing for attention. However, this constant influx of political communication has an unintended consequence: it desensitizes individuals, making them more susceptible to sophisticated phishing scams cleverly disguised amidst the chaos.

The Rise of Sophisticated Scams

Election phishing scams are not a new phenomenon, but they have evolved with alarming sophistication. Techniques such as smishing, vishing, spoofing and social media phishing have become increasingly refined, making it difficult for even the most cautious individuals to discern legitimate messages from fraudulent ones.

Smishing

A text message might innocently inquire about your voting preference, masquerading as a simple poll. However, responding to such messages can inadvertently verify your phone number for fraudsters, leading to more sinister attacks down the line, including SIM hijacking or malware scams.

Vishing

Perhaps more direct, vishing involves an attacker calling potential victims and pretending to be an election official or representative from a political campaign. These calls often request personal information or financial contributions. With the ability to "spoof" caller IDs, these scammers can make their attempts appear more legitimate than ever.

Spoofing

Beyond phone numbers, the internet is rife with spoofed web pages designed to mimic official platforms. These sites lure unsuspecting visitors with promises of voter registration updates, only to steal personal information or infect devices with malware.

Social Media Phishing

Social media platforms, with their vast networks and personal connections, are prime targets for fraudsters. Fake voter registration drives, malicious donation collections and the spread of misinformation are just the tip of the iceberg.

Protecting Yourself and Your Vote

While the threat of election phishing scams is real and present, there are several steps you can take to protect your organization:

Be Skeptical

Treat unsolicited messages with caution, regardless of how benign they may appear.

Verify Legitimacy

Always verify the sender's legitimacy before responding to any requests for personal information or financial contributions.

Avoid Suspicious Links

Never click on links from unknown sources, as they could lead to malicious websites.

Use Government Sources

For any election-related information, rely solely on verified government websites.

Report Suspicious Activity

If you encounter any suspicious messages or calls, report them to election officials immediately.

Consider Call-Blocking

Utilize call-blocking systems to filter out potential scam calls.

As we navigate through the murky waters of election season, let us arm ourselves with knowledge and vigilance. By understanding the tactics used by fraudsters and adopting safe practices in your organization, your personal information and the sanctity of your vote will be protected. Stay informed, stay skeptical and most importantly, stay safe. Together, we can ensure that our voices are heard, untainted by the efforts of those seeking to exploit the democratic process.

Electronic Payments Core of Knowledge

EPCOR is a not-for-profit payments association which provides payments expertise through education, advice and member representation. EPCOR assists banks, credit unions, thrifts and affiliated organizations in maintaining compliance, reducing risk and enhancing the overall operational efficiency of the payment systems. Through our affiliation with industry partners and other associations, EPCOR fosters and promotes improvement of the payments systems which are in the best interest of our members.
For more information on EPCOR, visit www.epcor.org.

Nacha® Direct Member

The Nacha Direct Member mark signifies that through their individual direct memberships in Nacha, Payments Associations are specially recognized and licensed providers of ACH education, publications and advocacy.

www.epcor.org
2345 Grand Blvd., Ste. 1700, Kansas City, MO 64108
800.500.0100 | 816.474.5630 | fax: 816.471.7665