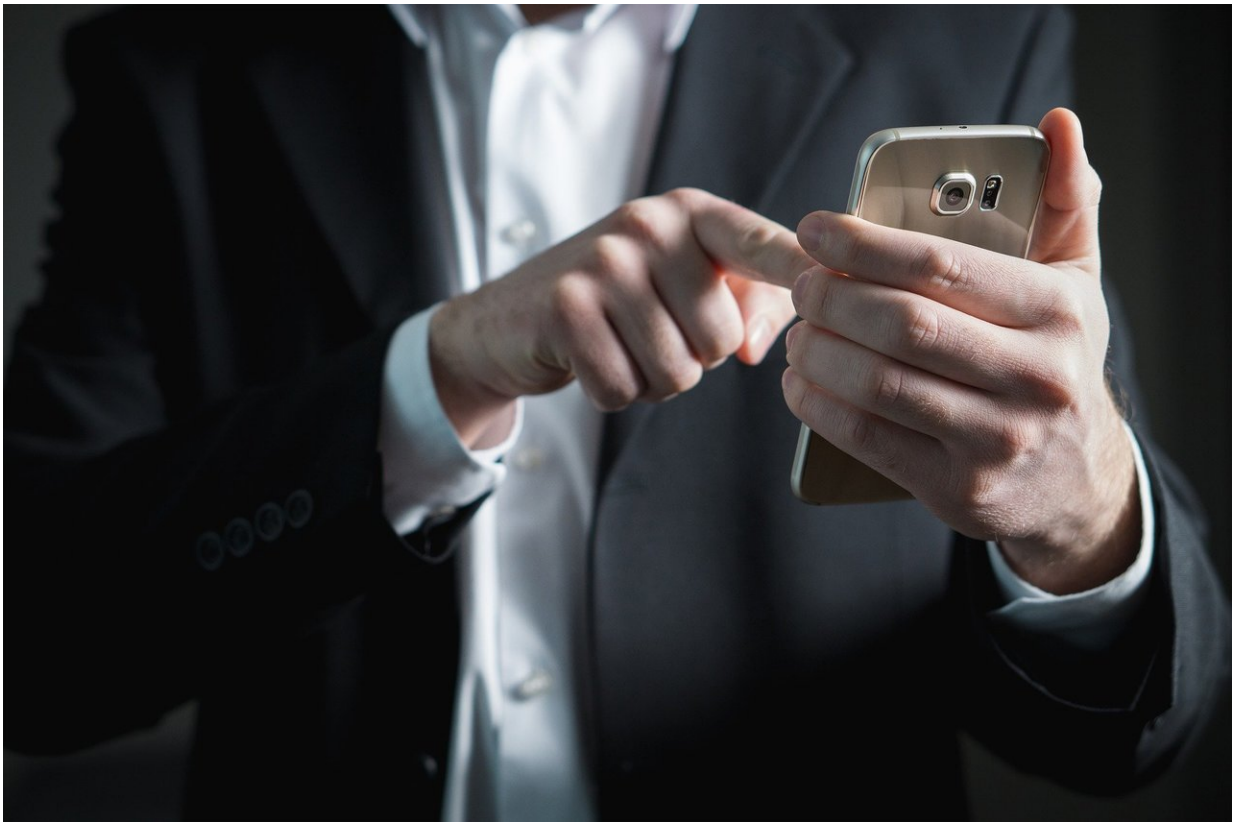
Email still beats texts—for hackers phishing for your data

February 27 2020, by Jefferson Graham



Credit: CC0 Public Domain

Despite all the attention given to phishing attacks, and high profile hacks, email still remains the number one place where victims fall prey to bad guys.

Business email getting compromised "is one of the oldest tricks in the book, and super effective," says Sam Small, the chief security officer for ZeroFOX, a firm that helps enterprises with security protection.

"You get an email, it looks and feels authentic, from someone you trust and they're asking you to do something," he adds. "The next thing you know, you've sent out a bogus wire transfer and the entire organization is at risk."

Hillary Clinton's 2016 campaign manager, John Podesta, was hacked after an authentic-looking email sent to his Gmail account asked him to confirm a link. From there, the campaign's emails were given to WikiLeaks and released to the world.

Earlier this year, we pointed out each telltale sign to look for in a phishing email, with a bogus one that arrived in our inboxes, supposedly from Chase bank.

Baltimore-based ZeroFOX, which is funded by several venture firms, including Intel's investment arm and NEA, helps companies inspect links for phishing attacks and the like. Small is attending the RSA Conference in San Francisco, where some 40,000 plus attendees, over 625 exhibitors and many speakers are here talking digital security, passwords, biometrics and how to keep consumers and office workers safe.

His advice to consumers: Check every link before you click on it. Write to the company directly to confirm that they sent it, or call.

Erich Kron, a "security awareness advocate," for KnowBe4, a Clearwater, Florida-based firm that trains employees about how to detect phishing attacks before it's too late, says email is "far and away the big one," due to volume.

We get more email than any other form of communication. "Think about it," he says. "You don't get as many texts or social media messages as you do with email. And it's really inexpensive to send them."

Services offer bulk email sends for as little as $65 for 50,000 emails, he adds. "Email addresses are easier to find than phone numbers. This is why they do it."

Your phone is the key—to everything

Mike Banic, the vice president of marketing for security firm Lookout is focused on protecting mobile devices, as opposed to laptops and desktops, since so much more of our work is being done on smartphones and tablets now.

"On mobile, it's not just email, it's everything. Facebook Messenger, LinkedIn, WhatsApp," he says. "It's everywhere."

Indeed, the smartphone belonging to Amazon CEO Jeff Bezos was likely hacked in 2019 by the Crown Prince of Saudi Arabia via a WhatsApp direct message, according to a United Nations investigation.

Lookout has a free smartphone app that says it automatically blocks phishing attempts and lets you "click confidently on links from Facebook, email, text messages and more."

However, the free app is very basic. Features like safe browsing, theft alerts and customer service start at $2.99 monthly and go to $9.99 monthly.

Ransomware attacks

Meanwhile, the other major security concern that's plaguing the nation, most notably cities, is ransomware. Cities like Baltimore, Atlanta and Greenville, North Carolina, recently found their public departments inoperable, when hackers got control of their systems and shut them down, demanding huge sums of money before they would agree to make them functional again.

The culprit here: not phishing, but basic digital sense, says Small. Cities, companies and consumers need to update their machines with software patches and improvements to keep the machines safer.

"This is a common problem a lot of organizations face," he says. "And it's totally avoidable."

More information: (c)2020 U.S. Today
Distributed by Tribune Content Agency, LLC.