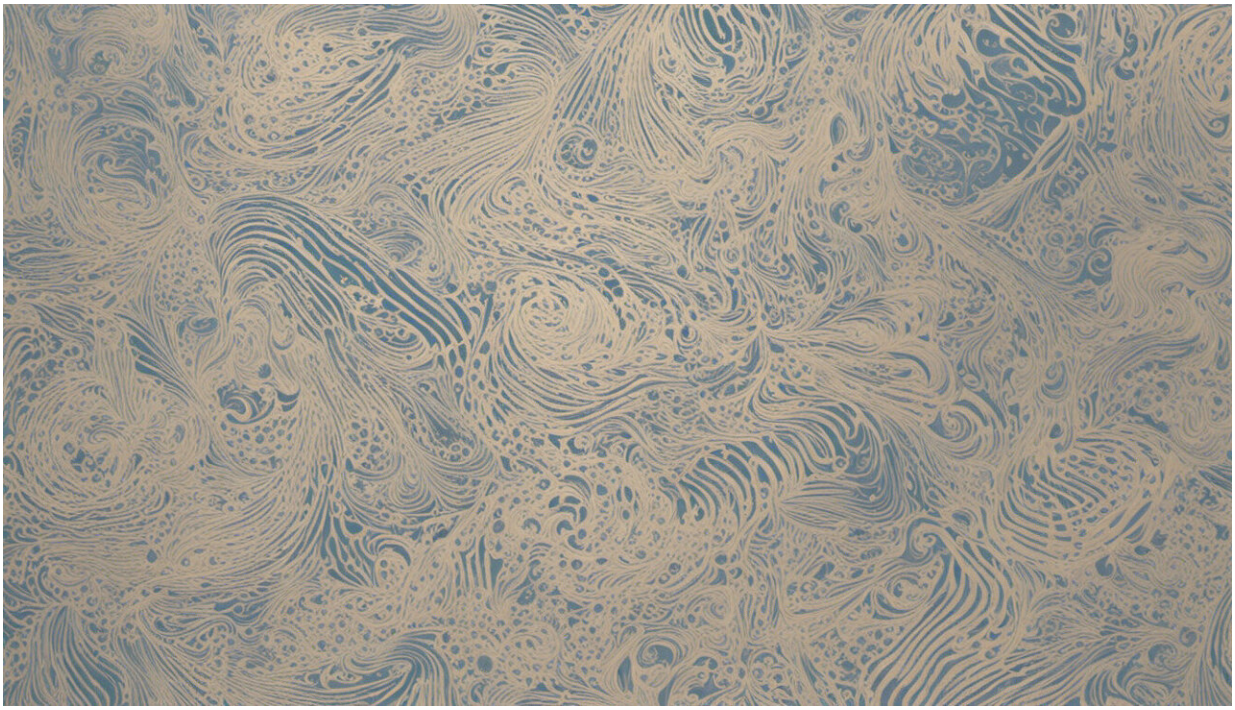
'Spearphishing' roiled the presidential campaign—here's how to protect yourself

November 8 2016, by Arun Vishwanath



Credit: AI-generated image (disclaimer)

Never in American political history have hacked and stolen emails played such a central role in a presidential campaign. But hackers are likely to target you as well – though perhaps with smaller repercussions for the world as a whole.

Every one of October's surprises, from the leaks of Clinton campaign chairman John Podesta's purported emails to those of the Democratic National Committee, was achieved using a surprisingly simple email deception technique called "spearphishing." The same technique was used to attack Hillary Clinton's private email server: Two spearphishing messages were found on it.

Many people know that the term "spearphishing" typically describes emails trying to get someone to click on a link to, say, their online bank account – but actually sending them to a lookalike site where their login information can be stolen. Some others hide malicious software (or "malware") within links or in attachments that when clicked give the attacker control of the system or even an entire corporate network.

But despite years of national efforts to promote cybersecurity, spearphishing remains fruitful: People are still the weakest links in cybersecurity defenses. There are, however, simple ways we can all step up to protect our own information – whether we're central to presidential politics or regular people.

A massively complex problem

In general, people are fairly aware of the potential for cyberattacks. Some are even good at spotting them. In fact, both Podesta and Clinton were suspicious of the phishing emails they received. Before clicking, Podesta even asked his tech-support staff if a link was legitimate. Those experts should have known how to spot a phishing attack, but failed: They told him to click on the malicious link.

The problem is not lack of awareness or even knowledge, though some of us need more of that too. It's actually one of complexity.

Researchers think of computer users as working on an email while

focused solely on a computer screen. But reality paints a different picture. Today, people use a variety of internet-connected gadgets and apps, with myriad prompts, feeds and notifications, all vying for their attention.

Estimates are that the average person checks his smartphone 80 to 100 times each day. This does not even include desktop and laptop computer screens, tablets or smartwatches. People routinely use all of those devices as well, checking, recording, reviewing and responding to requests in the office and on the go – walking, talking and even driving.

These interactions present a near-constant stream of information and requests. The user typically feels that he has just seconds to consider each – even though any one of them could define the fate of an entire organization or a political campaign.

A very simple solution

In the face of all this complexity, the best answer is a very simple one: a checklist.

Atul Gawande, in his book "The Checklist Manifesto: How to Get Things Right," details the importance of checklists in highly specialized fields. These are work environments where success depends on coordination between a number of trained professionals – airline pilots, surgical teams, construction engineers. Often, trained people remember to do complex tasks, like medical professionals performing difficult surgical procedures, but forget to do simple things, like washing hands prior to surgery.

Much like in cybersecurity, the problem is one of complexity and human error, with potentially severe consequences. For instance, one in every 200 medical errors involves performing the wrong procedure, or even

working on the wrong patient. That's where a checklist comes in, reminding the medical staff to reconfirm the patient's name and visibly mark the correct surgical site.

In much the same way, a checklist could help us routinize the minimum actions necessary for achieving cybersafety. With this goal in mind, here is a checklist of five best practices that could help protect us online.

Five steps to more secure online operations

1. Enable two-factor authentication (2FA). Most major online services, from Amazon to Apple, today support 2FA. When it's set up, the system asks for a login and password just like usual – but then sends a unique numeric code to another device, using text message, email or a specialized app. Without access to that other device, the login is refused. That makes it much harder to hack into someone's account – but users have to enable it themselves.
2. Encrypt your internet traffic. A virtual private network (VPN) service encrypts digital communications, making it hard for hackers to intercept them. Everyone should subscribe to a VPN service, some of which are free, and use it whenever connecting a device to a public or unknown Wi-Fi network.
3. Tighten up your password security. This is easier than it sounds, and the danger is real: Hackers often steal a login and password from one site and try to use it on others. To make it simple to generate – and remember – long, strong and unique passwords, subscribe to a reputable password manager that suggests strong passwords and stores them in an encrypted file on your own computer.
4. Monitor your devices' behind-the-scenes activities. Many computer programs and mobile apps keep running even when they are not actively in use. Most computers, phones and tablets

have a built-in activity monitor that lets users see the device's memory use and network traffic in real time. You can see which apps are sending and receiving internet data, for example. If you see something happening that shouldn't be, the activity monitor will also let you close the offending program completely.

5. Never open hyperlinks or attachments in any emails that are suspicious. Even when they appear to come from a friend or coworker, use extreme caution – their email address might have been compromised by someone trying to attack you. When in doubt, call the person or company directly to check first – and do so using an official number, never the phone number listed in the email.

Even using this checklist can't guarantee stopping every attack or preventing every breach. But following these steps will make it significantly harder for hackers to succeed. And it will help us all develop security consciousness and ultimately better cyberhygiene. Our leaders could certainly use the help.

This article was originally published on The Conversation. Read the original article.

Provided by The Conversation

Citation: 'Spearphishing' roiled the presidential campaign—here's how to protect yourself (2016, November 8) retrieved 23 April 2024 from https://phys.org/news/2016-11-spearphishing-roiled-presidential-campaignhere.html