

How we can each fight cybercrime with smarter habits

January 26 2015, by Arun Vishwanath



Something weird in the inbox? Credit: Martin Terber, CC BY

Hackers gain access to computers and networks by exploiting the weaknesses in our cyber behaviors. Many attacks use simple phishing schemes – the hacker sends an email that appears to come from a trusted source, encouraging the recipient to click a seemingly innocuous hyperlink or attachment. Clicking will launch malware and open

backdoors that can be used for nefarious actions: accessing a company's network or serving as a virtual zombie for launching attacks on other computers and servers.

No one is safe from such [attacks](#). Not companies at the forefront of technology such as Apple and Yahoo whose security flaws were recently exploited. Not even sophisticated national networks are home free; for instance, Israel's was compromised using a [phishing attack](#) where an email purportedly from Shin Bet, Israel's internal security service, with a phony PDF attachment, gave hackers remote access to its defense network.

To figure out why we fall for hackers' tricks, I use them myself to see which kinds of attacks are successful and with whom. In my research, I simulate real attacks by sending different types of suspicious emails, friend-requests on [social media](#), and links to spoofed websites to research subjects. Then I use a variety of direct, cognitive and psychological measures as well as unobtrusive behavioral measures to understand why individuals fall victim to such attacks.

What is apparent over the many simulations is how seemingly simple attacks, crafted with minimal sophistication, achieve a staggering victimization rate. As a case in point, merely incorporating the university's logo and some brand markers to a phishing email resulted in [close to 70%](#) of the research subjects falling prey to the attack. Ultimately, the goal of my research is to figure out how best to teach the public to ward off these kinds of cyberattacks when they come up in their everyday lives.

Clicking without thinking

Many of us fall for such deception because we misunderstand the risks of online actions. I call these our cyber-risk beliefs; and more often than

not, I've found people's risk beliefs are inaccurate. For instance, individuals mistakenly equate their inability to manipulate a PDF document with its inherent security, and quickly open such attachments. Similar flawed beliefs lead individuals to cavalierly open webpages and attachments on their mobile devices or on certain operating systems.

Compounding such beliefs are people's email and social media habits. Habits are the brain's way of automating repeatedly enacted, predictable behaviors. Over time, frequently checking email, social media feeds and messages becomes a routine. People grow unaware of when – and at times why – they perform these actions. Consequently, when in the groove, people click links or open attachments without much forethought. In fact, I've found certain [Facebook habits](#) – such as repeatedly checking newsfeeds, frequently posting status updates, along with maintaining a large Facebook friend network – to be the biggest predictor of whether they would accept a friend-request from a stranger and whether they would reveal personal information to that stranger.

Such habitual reactions are further catalyzed by the [smartphones and tablets](#) that most of us use. These devices foster quick and reactive responses to messages through widgets, apps and push notifications. Not only do smartphone screen sizes and compressed app layouts reduce the amount of detailed information visible, but many of us also use such devices while on the go, when our distraction further compromises our ability to detect deceptive emails.

These automated cyber routines and reactive responses are, in my opinion, the reasons why the current approach of training people to be vigilant about suspicious emails remains largely ineffective. Changing people's media habits is the key to reducing the success of cyberattacks—and therein also lies an opportunity for all of us to help.

Harnessing habits to fight cybercrime

Emerging research suggests that the best way to correct a habit is to replace it with another, what writer Charles Duhigg calls a [Keystone Habit](#). This is a simple positive action that could replace an existing pattern. For instance, people who wish to lose weight are instructed to exercise, reduce sugar intake, read food labels and count calories. Doing this many challenging things consistently is daunting and often people are too intimidated to even begin. Many people find greater success when they instead focus on one key attainable action, such as walking half a mile each day. Repeatedly accomplishing this simple goal feels good, builds confidence and encourages more cognitive assessments—processes that quickly snowball into massive change.

We could apply the same principle to improve cybersecurity by making it a keystone habit to report suspicious emails. After all, many people receive such emails. Some inadvertently fall for them, while many who are suspicious don't. Clearly, if more of us were reporting our suspicions, many more breaches could be discovered and neutralized before they spread. We could transform the urge to click on something suspicious into a new habit: reporting the dubious email.

We need a centralized, national clearing house—perhaps an email address or phone number similar to the 911 emergency system—where anyone suspicious of a cyberthreat can quickly and effortlessly report it. This information could be collated regionally and tracked centrally, in the same way the Department of Health tracks public health and disease outbreaks.

Of course, we also need to make reporting suspicious cyber breaches gratifying, so people feel vested and receive something in return. Rather than simply collect emails, as is presently done by the many different institutions combating cyber threats, submissions could be vetted by a centralized cybersecurity team, who in addition to redressing the threat, would publicize how a person's reporting helped thwart an attack.

Reporting a cyber intrusion could become easy, fun, something we can all do. And more importantly, the mere act of habitually reporting our suspicions could in time lead to more cybersecurity consciousness among all of us.

This story is published courtesy of [The Conversation](#) (under Creative Commons-Attribution/No derivatives).

Source: The Conversation

Citation: How we can each fight cybercrime with smarter habits (2015, January 26) retrieved 27 April 2024 from <https://phys.org/news/2015-01-cybercrime-smarter-habits.html>

<p>This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.</p>
--