Protect your WEAKEST SECURITY LINK —end users

A GUIDE TO DEFENDING AGAINST SOCIAL ENGINEERING ATTACKS

AMATEURS HACK SYSTEMS. PROFESSIONALS HACK PEOPLE.

—Bruce Schneier, CTO
Counterpane Internet Security, Inc.[1]

2015 MARKED AN IMPORTANT YEAR in the world of network security. For the first time, social engineering attacks outnumbered attacks on software vulnerabilities and exploits. This is a serious problem.

For companies to stay productive, they need employees to be able to work from anywhere on any device, often collaborating with people around the world. This mobility drives not only the need for secure file sharing and email accounts but also a fundamental shift in our approach to computer security.

Since January 2015, the number of victims identified by the FBI has increased 270%, costing businesses more than $2.3 billion[2]. The message to network security professionals is clear. Hackers are targeting the weakest link in any security perimeter—the end user.

This book is your guide to helping you detect and prevent social engineering attacks, and to better understand how to defend your company from what has grown to become the dominant global cyberthreat.

what is

SOCIAL ENGINEERING?

Social engineering happens when someone uses manipulation, influence or deception to get another person to release information or to perform some sort of action that benefits a hacker.

Hackers will often take advantage of genuine security gaps in your network. But at organizations of any size, layers of sophisticated computer security can be undone in seconds because one employee—whether because of trust, lack of awareness, or carelessness—reveals company information to someone with malicious intent.

Your employees could be tricked into anything from allowing someone to tailgate them into your data center to giving up their passwords or user IDs over the phone. Social engineers go to great lengths to gain access to data they can exploit, such as:

- **PERSONAL INFO**
  passwords, account numbers
- **COMPANY INFO**
  phone lists, identity badges
- **SERVER INFO**
  servers, networks, non-public URLs

Familiarizing yourself with social engineering techniques is your first line of defense.

So, what does a social engineer sound like?

You might believe that social engineers would be easy to spot. But often enough, they sound like people you run into at work every day.

ON THE PHONE

"This is Kevin from IT. We've been notified of a virus on your department's machines."

One of the most common scams—a hacker poses as an IT help desk worker to glean sensitive info such as a passwords from an unsuspecting employee.

AT THE RECEPTION DESK

"Hi, I'm the service tech from HP and I think Ellen is expecting me at 1pm."

This is why it's so important that well-meaning staff members and other insiders need to be educated as to how and why they could be targeted—and what to do if they suspect a potential threat.

AT THE BUILDING ENTRANCE

"Oh! Wait, could you please hold the door? I left my key/access card in my car."

People want to be helpful, and they often downplay the risks of engaging with someone they don't know—and that can be a perilous mix.

tactic no. 1

SPEAR PHISHING

Spear phishing is a targeted email attack in which a hacker uses email to masquerade as someone the target knows and trusts. This is often as simple as copying the name of a CEO from a company website and then sending an email using this name to anyone on the company's corporate domain.

Spear phishing is the single most common (and effective) social engineering tactic. You've likely seen subject lines like these before and hopefully hit "delete" right away:

"Notice of pending layoff: Click here to register for severance pay."

"In an effort to cut costs, we're sending this year's W-2s electronically."

But hackers are getting more convincing and creative with email that, when opened, infects your machine. Here are a few tactics to watch for...

- **USING THE NEWS AGAINST YOU** – Whatever's getting attention in the news can be used as social engineering lures. For example, 2016 has seen a rise in the number of spam messages related to the presidential campaign.

- **ABUSING FAITH IN SOCIAL NETWORKING SITES** – Millions of people use social networking sites like Facebook and LinkedIn daily, so they develop a certain trust in them. Then, when an email says, "Your Facebook account is undergoing routine maintenance, please click to update your information," you don't think twice before you click.

tactic no. 2

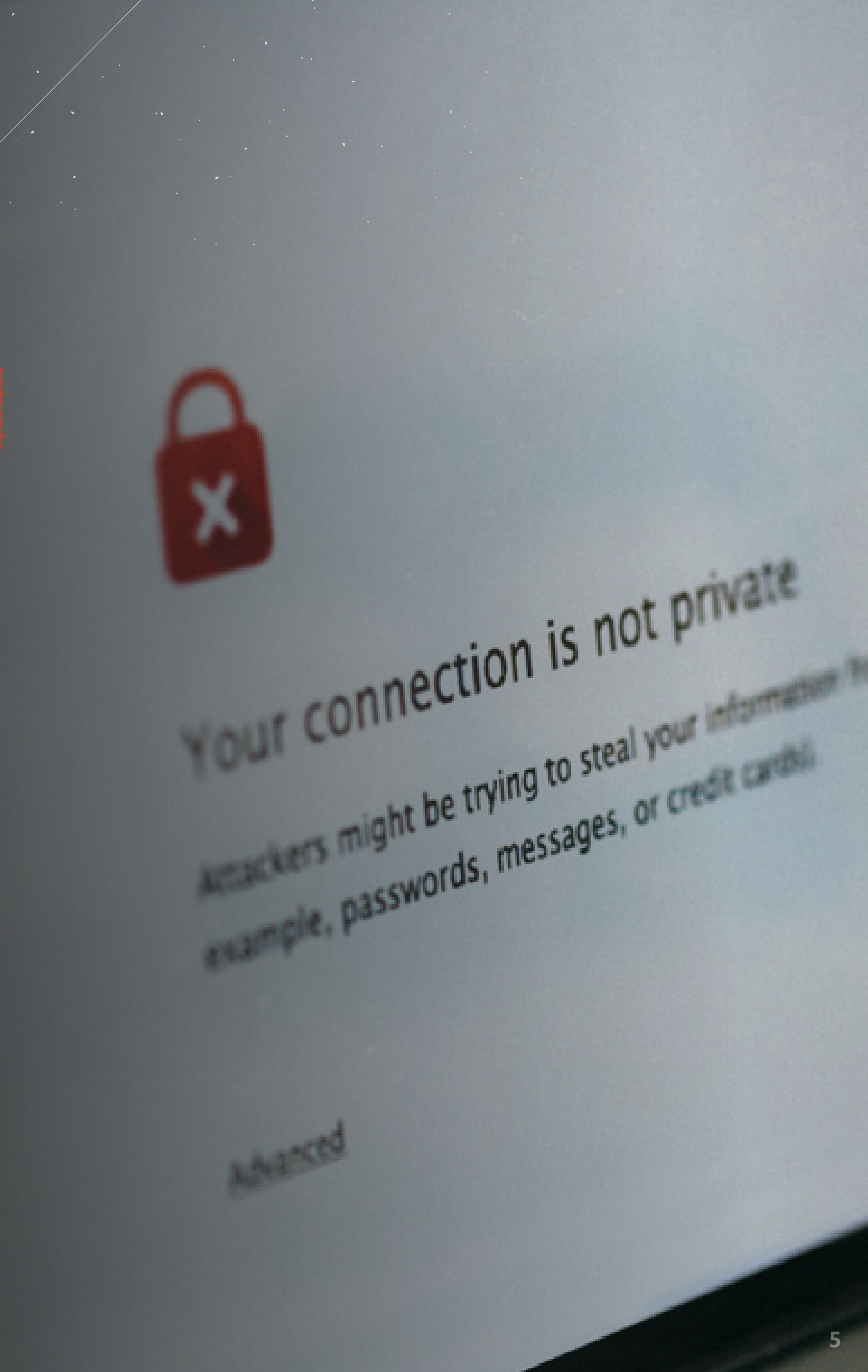
DUMPSTER DIVING

Dumpster diving is exactly what it sounds like: A hacker digs through the trash that unsuspecting employees have thrown away. Valuable finds might include:

- Junk mail (especially credit card offers), which can contain personal identification info that's just the ticket to identity theft.
- Company phone lists and org charts that offer numbers and locations that make it easier to impersonate management-level team members.
- Corporate letterhead that can be used to fake official-looking correspondence.
- Hackers will also buy refurbished computers and will pull confidential information from hard drives, even after users think they have deleted it.

CYBER CRIME HOLDS THE POTENTIAL TO CRIPPLE BUSINESSES.

—Steven R. Chabinsky, Deputy Assistant Director, Cyber Division
Federal Bureau of Investigation[3]



Your connection is not private

Attackers might be trying to steal your information f

example, passwords, messages, or credit cards).

Advanced

tactic no. 3

10° OF SEPARATION

Social engineers are clever, methodical, and patient. They often start by building a rapport with more accessible people in an organization—like an administrative assistant or a guard at the gate—to get information about their ultimate target, who may be as many as ten steps higher up on the corporate food chain.

The criminal may begin by gathering personal nuggets about team members, as well as other "social cues" to build trust or even successfully masquerade as an employee. Some of their strategies are incredibly simple, and insidious:

- **THEY LEARN YOUR INDUSTRY SHORTHAND**–A hacker will study the acronyms and jargon of your industry so she can build trust by speaking the language you recognize.
- **THEY BORROW YOUR 'HOLD' MUSIC** – In this deceptively simple scheme, the criminal calls, gets put on hold, and records the music. Then, when he calls his victims and puts them on hold, the familiar music serves as a psychological cue that the caller is trustworthy and on the inside.
- **THEY SPOOF YOUR PHONE NUMBER** – Criminals make an inside number show up on the victim's caller ID, which makes the victim more willing to offer confidential information like passwords over the phone.

let's talk about IMPACT

Legendary programmer and developer of the first commercial antivirus program, John McAfee has said, "Social engineering has become about 75% of an average hacker's toolkit, and for the most successful hackers, it reaches 90% or more[4]." Clearly, social engineering is a very real problem with very few real solutions. In addition to the obvious financial toll, a company's reputation can take a major hit when a hack becomes public. Compromised personal data can erode the faith and goodwill of its customer base—and that too affects the bottom line. Here's what we know...

1 *Attackers are increasingly infecting computers by tricking people into doing it themselves*

A mind-blowing 99.7% of docs used in attachment-based campaigns relied on social engineering and macros. And 98% of URLs in malicious messages link to hosted malware.[5]

2 *On social media, phishing is 10 times more likely than malware*

Because creating fake social media accounts for known brands is so easy, phishing is the fastest growing social media threat. Distinguishing the fraudulent from the legitimate is tough too: 40% of accounts claiming to represent Fortune 100 companies on Facebook and 20% on Twitter are unauthorized.[6]

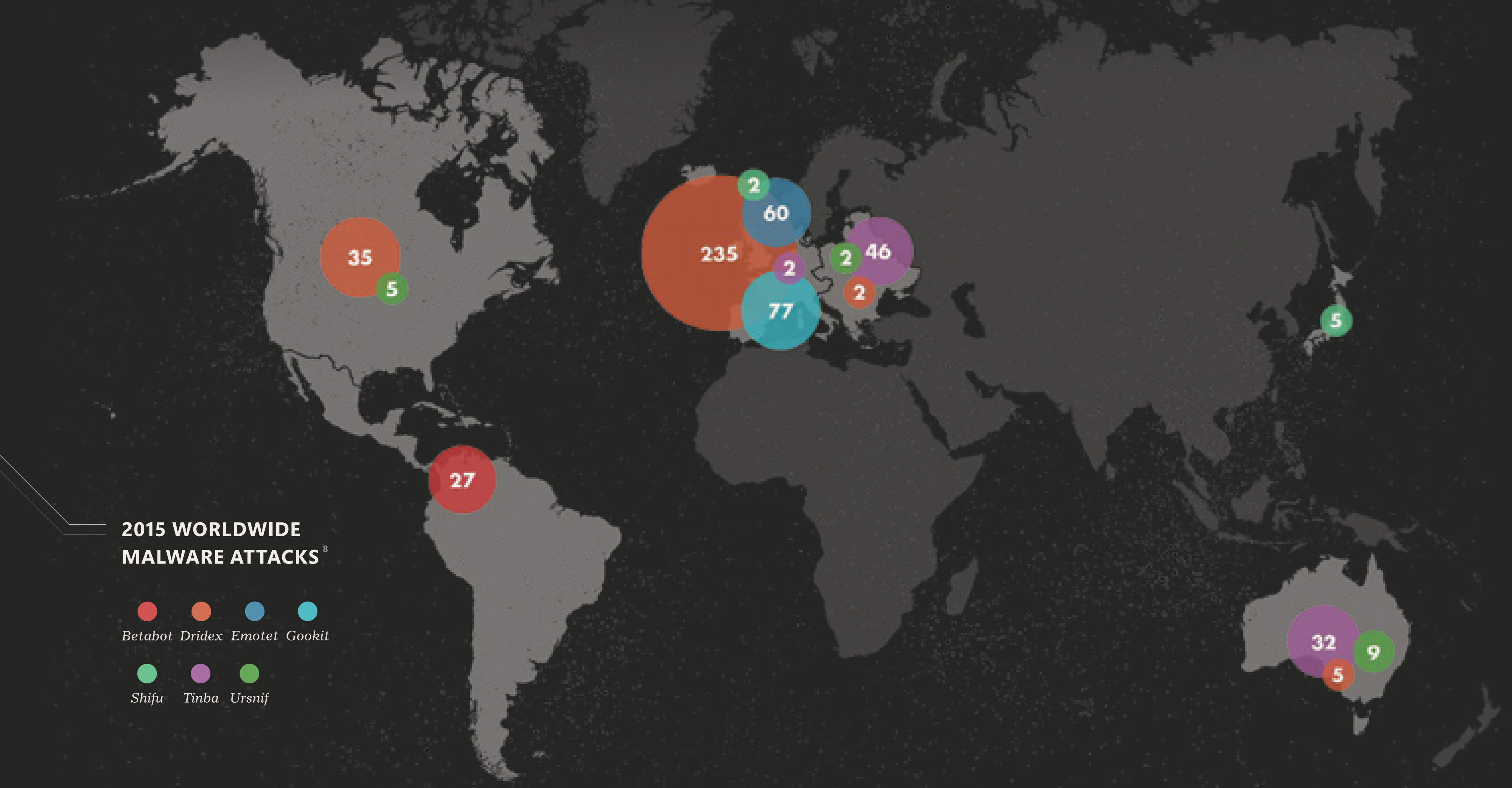
3 *More than 2 billion mobile apps that steal personal data have been willingly downloaded*

Email and social media are not the only social engineering playgrounds—these criminals do big business via malicious mobile apps too. More than 12,000 have been discovered in app stores alone.[7]

social engineering attacks

HAVE GONE GLOBAL

No country is immune to social engineering attacks, no matter how sophisticated its technology. This graphic shows the distribution of top social engineering campaigns by geographical region.



2015 WORLDWIDE MALWARE ATTACKS[8]

how do you PROTECT YOUR ORGANIZATION?

Social engineering is an undeniable and potentially disastrous reality. So, what can organizations like yours do proactively to protect your vulnerable people and keep valuable data out of the hands of scam artists with intent to do harm?

REAL-WORLD PREVENTION STRATEGIES

What follows is a list of tangible changes you can make and security policies you can implement that can help. But remember, for any of this work to be effective, education is absolutely crucial. To mitigate your risk, start with new-employee training and follow through with regular threat assessments, policy updates, and company-wide reviews. Also keep communication open and your team members well informed.

Clearly articulate an easy-to-understand security policy, which includes:

- Password management – Outline rigorous standards for secure passwords and insist on regular expiration and change. Also ensure careful onsite and remote access authorization and accountability.

- Two-factor authentication – Use two-factor authentication rather than fixed passwords to authenticate high-risk network services like VPNs.

- Antivirus/anti-phishing defenses – Layers of the latest antivirus defenses at vulnerable locations like mail gateways and end-user desktops aren't going to solve the problem, but they're a good place to start.

- Change management – When your team is comfortable and familiar with a well-documented change-management process (rather than reacting off the cuff), they're less vulnerable to an attack that relies on a false sense of urgency.

- Information classification – Ensure that confidential information is clearly called out and handled as such.

- Document destruction – Confidential info should be shredded rather than tossed into the trash or recycling.

- Physical security – Controls such as visitor logs, electronic security devices, escort requirements, and background checks are key to a comprehensive security policy.

Build a security-aware culture

- Promote an awareness of threats and risky behavior – Educating employees on the real-world damage done by such theft to other companies is particularly impactful.

- Empower employees to recognize threats and make smart security decisions on their own – Because social engineering tactics change so frequently, fostering a sensitivity to risk and the tools for addressing it immediately and locally is key.

- Embed security awareness deeply in the minds of your team members – You've probably heard of the "see something/ say something" anti-terrorism campaign. Likewise, to counter cyber attacks of all kinds, ensure that employees at every organizational level feel comfortable with reporting anything suspicious.

THERE ARE TWO TYPES OF COMPANIES: THOSE THAT HAVE BEEN HACKED, AND THOSE WHO DON'T KNOW THEY HAVE BEEN HACKED.

—John Chambers, CEO
Cisco[9]

what's NEXT?

> YOUR EMPLOYEES COULD BE THE BIGGEST RESOURCE YOU HAVE TO PROTECT YOUR SYSTEMS.
>
> *—Brian Chappell, Director of Technical Services EMEAI and APAC Identity management firm BeyondTrust*[10]

First of all, no matter how strong your technical security is, your organization's people are often the most vulnerable link in the chain. But, with thorough, thoughtful, and regular education, they can also be your biggest asset in your fight against social engineering. However, this is only possible when every individual in the organization clearly understands the very real risks, the strategies that can offer protection, and the big-picture goals and limitations of enterprise security.

Finally, because the fight against social engineering is so complex and challenging, no ONE suggestion or strategy outlined here will guarantee security. But, by proactively attacking the problem from all sides, adopting viable prevention strategies, and promoting a security-aware culture, you can help to protect your organization, your data, and your people from this insidious 21st century threat.

ALL OVER THE GLOBE, SOCIAL ENGINEERING IS A DOMINANT AND GROWING THREAT TO ORGANIZATIONAL SECURITY.

Microsoft invests over $1 billion a year in cybersecurity research, and has developed a state-of-the-art Cyber Defense Operations Center, that brings together security response experts from across the company to help protect, detect and respond to threats in real time.

Microsoft

1. Bruce Schneier, CTO, Counterpane Internet Security, Inc.
   http://www.iwar.org.uk/comsec/resources/sa-tools

2. 9th Annual Report. Information Security Trends. ComTIA
   https://www.comptia.org/resources/9th-annual-information-security-trends

3. Steven R. Chabinsky, Deputy Assistant Director, Cyber Division, Federal Bureau of Investigation
   https://archives.fbi.gov/archives/news/speeches/the-cyber-threat-whos-doing-what-to-whom

4. John McAfee
   http://www.ibtimes.co.uk/john-mcafee-death-antivirus-1507388

5. Proofpoint Report, 2016. The Human Factor

6. Research Paper: The State of Social Media Infrastrucutre. NextGate

7. Proofpoint Report, 2016. The Human Factor

8. (Map) Proofpoint Report, 2016. The Human Factor

9. Cisco CEO John Chambers
   http://www.networkworld.com/article/2952184/cisco-subnet/john-chambers-10-most-memorable-quotes-as-cisco-ceo.html

10. Brian Chappell, Director of Technical Services EMEAI and APAC. BeyondTrust
   http://www.information-age.com/technology/security/123460760/2016-cyber-security-roadmap