

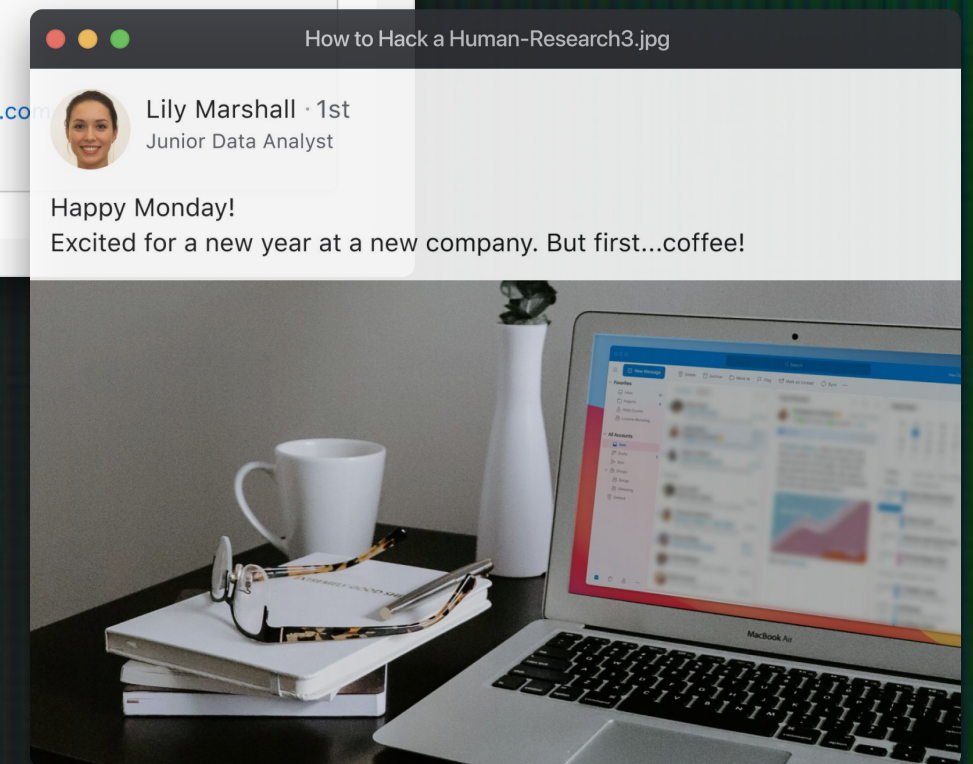
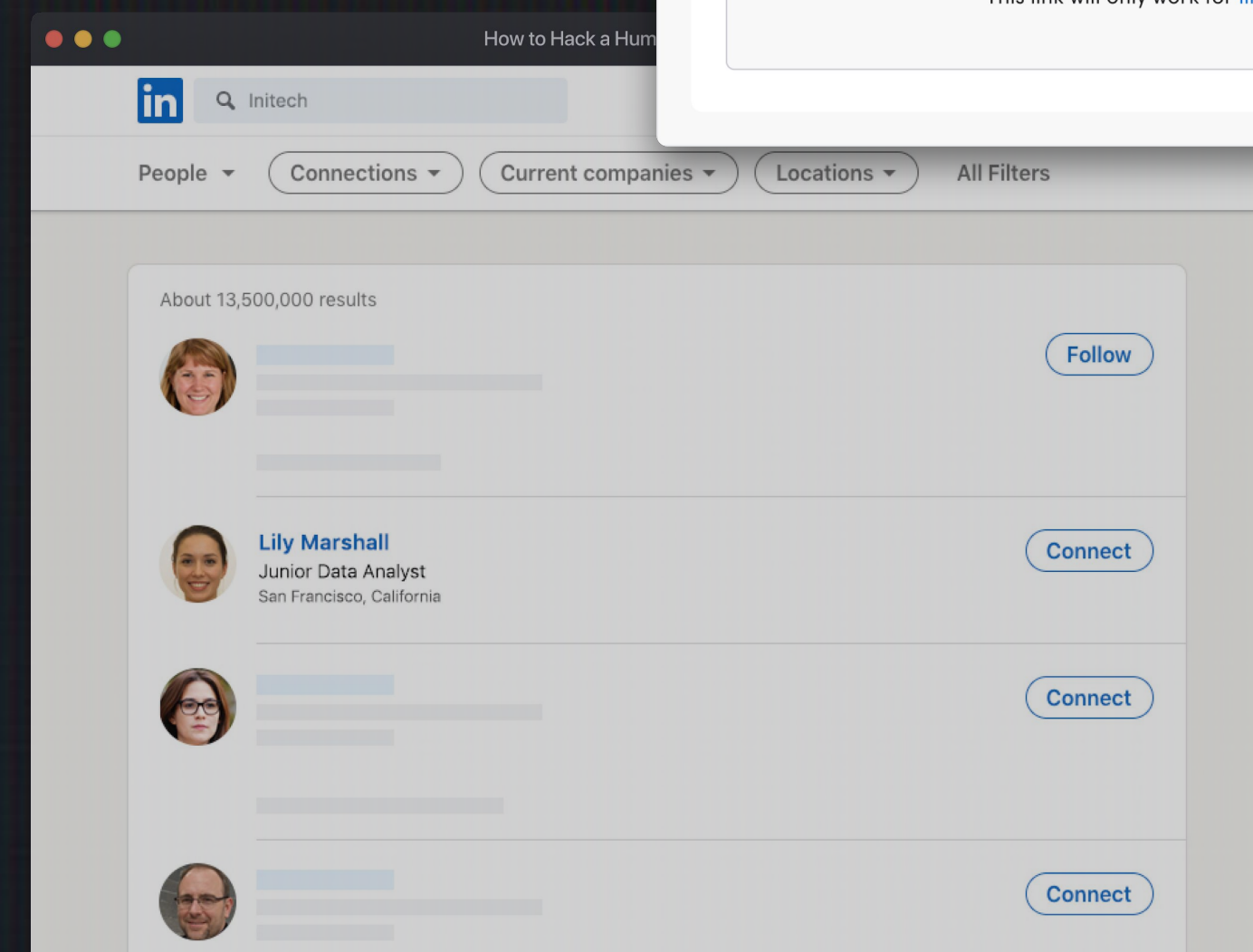
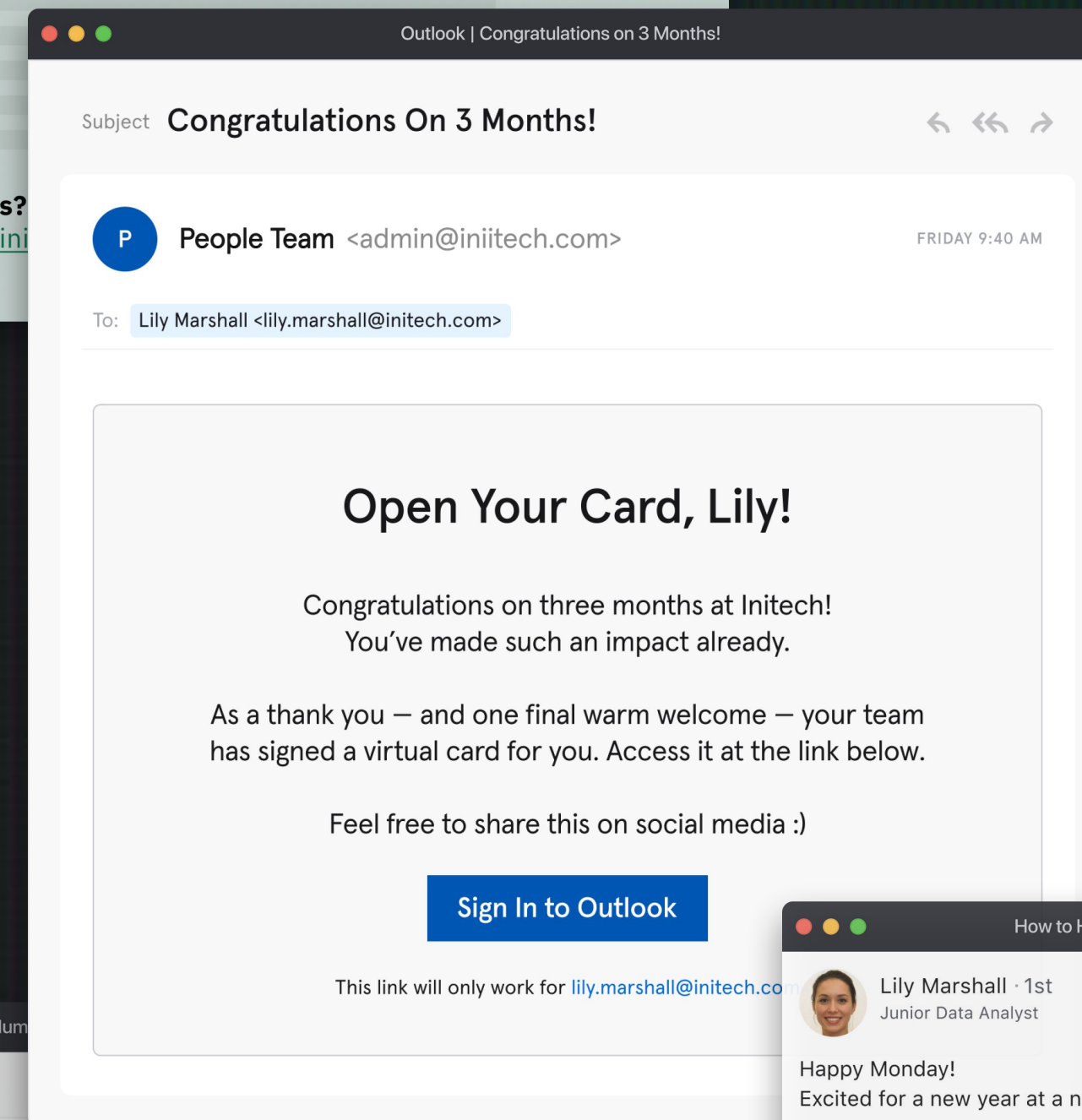
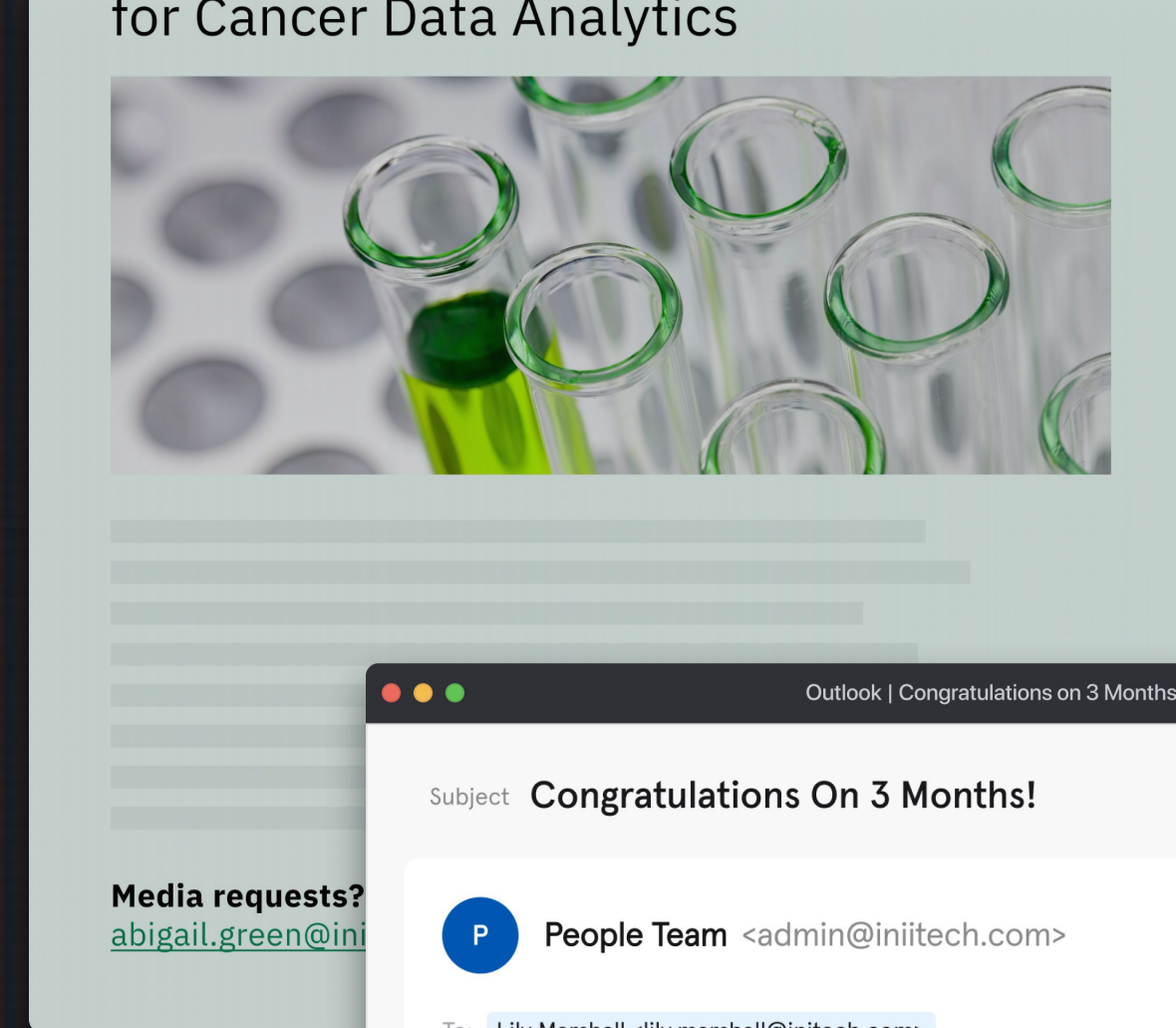


SOCIAL MEDIA | SOCIAL ENGINEERING | BUSINESS EMAIL COMPROMISE

//how to hack a human

Every photo we post, status we update, person we tag, and place we check into reveals valuable information about our personal and professional lives. And hackers use this information to craft targeted — and effective — social engineering attacks *at scale*. Learn how.

Share this report





[Jump to Page 6 ↗](#)

90%

of people post information related to their personal and professional lives online.



93%

of employees update social media profiles when they get a new job.

[Jump to Page 11 ↗](#)



77%

of people reuse passwords.

[Jump to Page 17 ↗](#)



88%

of people have received a suspicious message or link in the last year.

[Jump to Page 19 ↗](#)



55%

of people have public accounts.



32%

of employees post business travel photos and updates.

[Jump to Page 8 ↗](#)



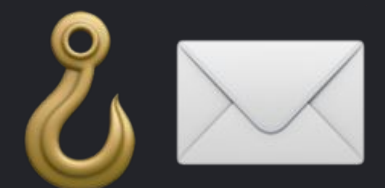
42%

of people post on social media every day.

[Jump to Page 11 ↗](#)

Email

is the #1 threat vector for social engineering.



[Jump to Page 19 ↗](#)



URGENT – Wire Transfer

Hi Kim,

Sorry to bother you while you're on holiday, but there's an urgent wire transfer I need you to approve.

Introduction

Over the last decade, phishing – a type of social engineering attack – has transformed from something more like spam to the threat most likely to cause a breach.

During that same period, the number of adults on social media platforms like Facebook increased by almost 1,300%.

Every photo we post, status we update, person we tag, and place we check into reveals valuable information about our personal and professional lives. And hackers use this information to craft targeted – and effective – social engineering attacks *at scale*.

In this report, we explore how hackers hack humans *and* businesses by exploiting two key vulnerabilities:

- ① The average person shares *a lot* of information online
- ② The average person isn't a security expert



The Attack

Lily Marshall · 1st
Junior Data Analyst

Happy Monday!
Excited for a new year at a new company. But first...coffee!

The Attack

Andrew Neal · 1st
Chief Financial Officer at SoBank

I'm so excited to be joining @CliffordTucker @TaylorMac, and so many others tomorrow for @MoneyTalks2021. See you in Boston on March 8!

Andrew Neal
Chief Financial Officer
SoBank

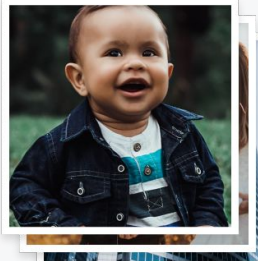
Money Talks 2021
Boston, March 8

The Attack


izza_o12g

Table of contents

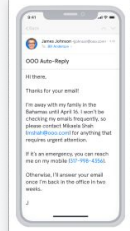
How to Hack a Human — Part 1



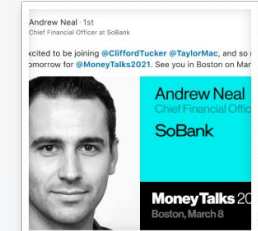
The social network.jpg



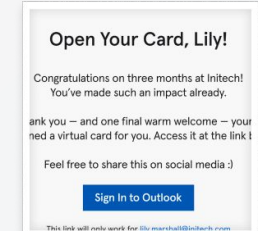
Hackers hack humans to hack the companies they work for.jpg




OOO? TMI.jpg



Social Engineering Example 1.jpg



Social Engineering Example 2.jpg



Not-so-strong passwords.jpg

Thumbnail

Part 1

Your digital footprint = a hacker's toolkit

pg. 5

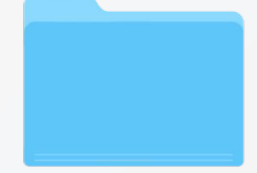
Thumbnail

Part 2

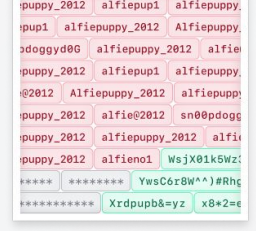
How to level-up your email security

pg. 14

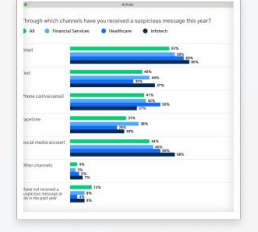
How to Hack a Human — Part 2




A hacker's toolkit.jpg




We're not all security experts.jpg



Does this look suspicious to you?.jpg



Do's and don'ts.jpg



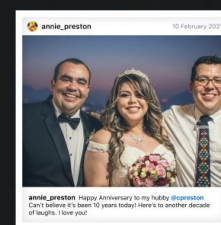
Tessian Solutions.jpg

Part 1

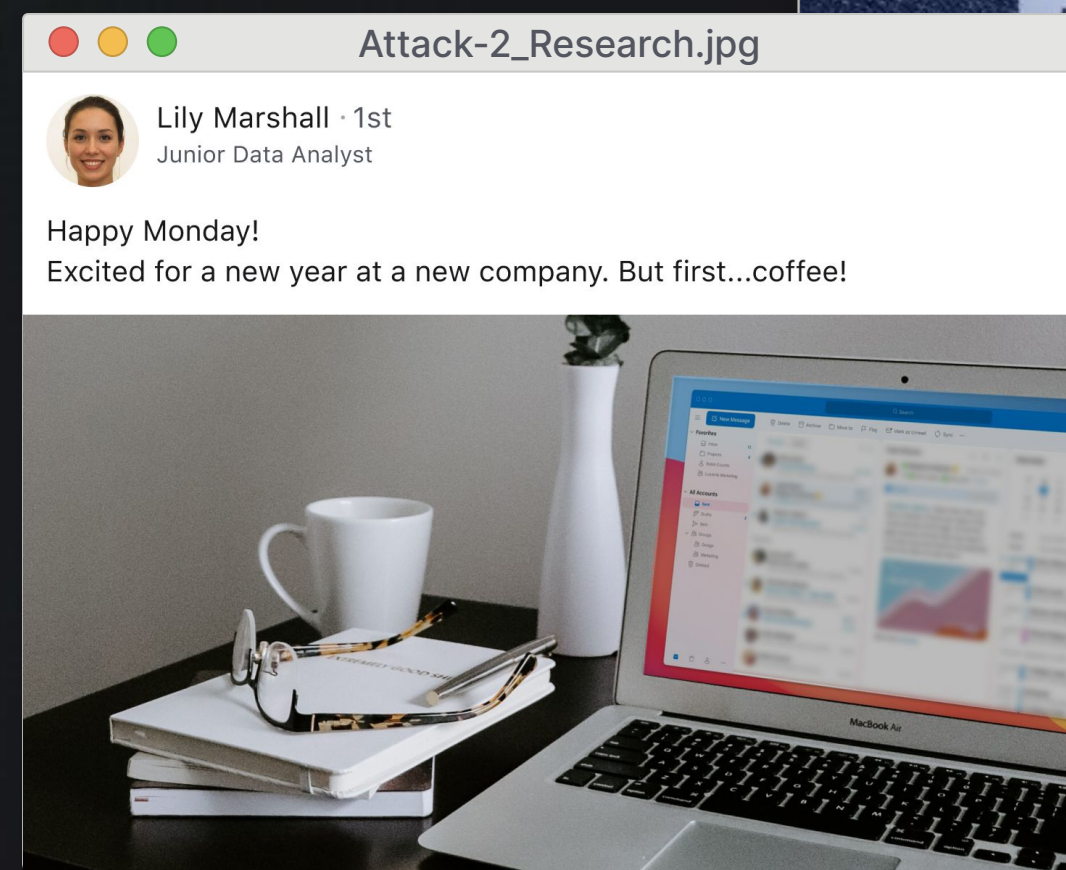
Your digital footprint = a hacker's toolkit



The social network.jpg

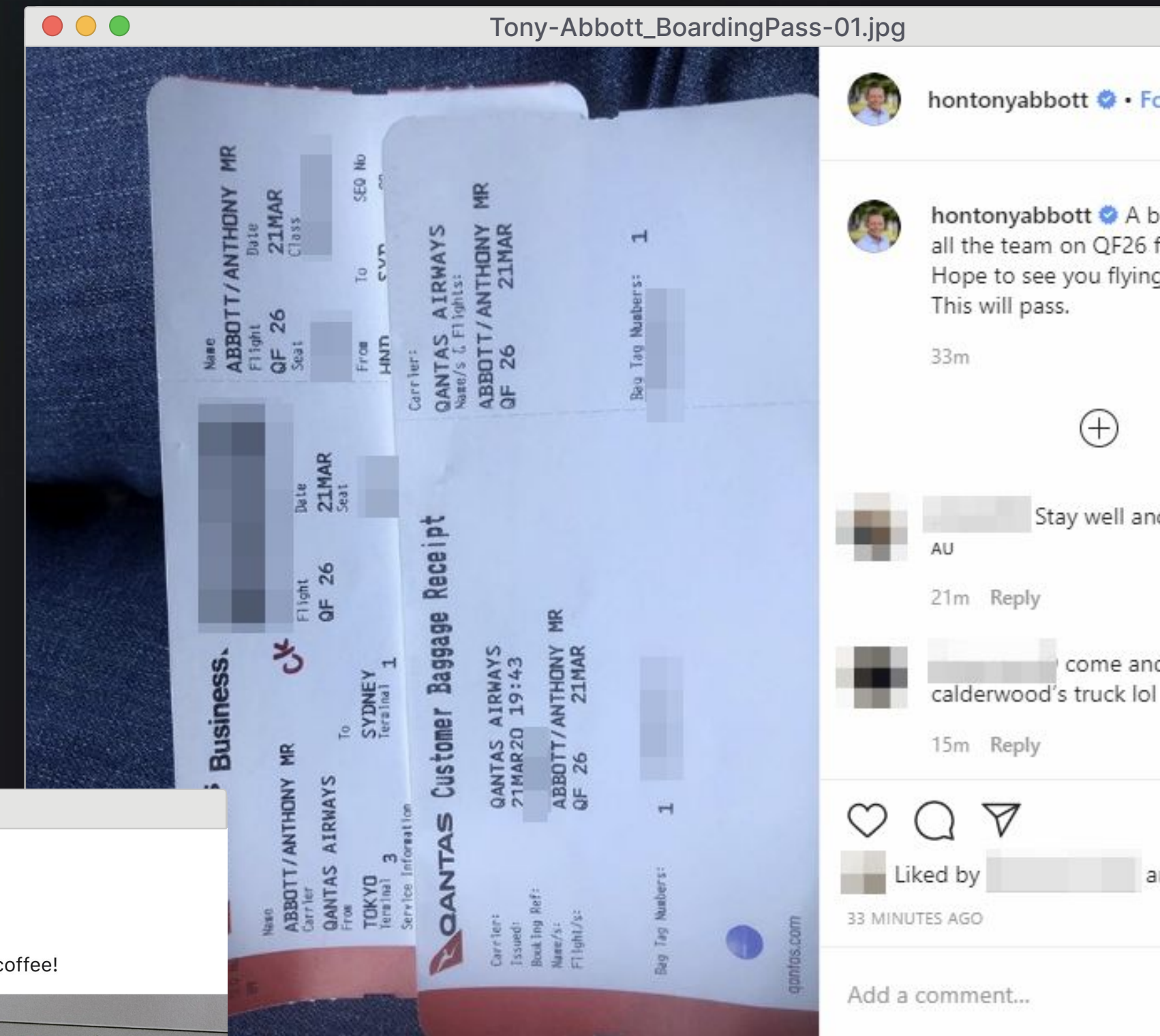


Not-so-strong passwords.jpg



Lily Marshall · 1st
Junior Data Analyst

Happy Monday!
Excited for a new year at a new company. But first...coffee!



Tony-Abbott_BoardingPass-01.jpg

hontonyabbott · Follow

hontonyabbott · A b
all the team on QF26 f
Hope to see you flying
This will pass.

33m

Stay well and
AU

21m Reply

come and
calderwood's truck lol

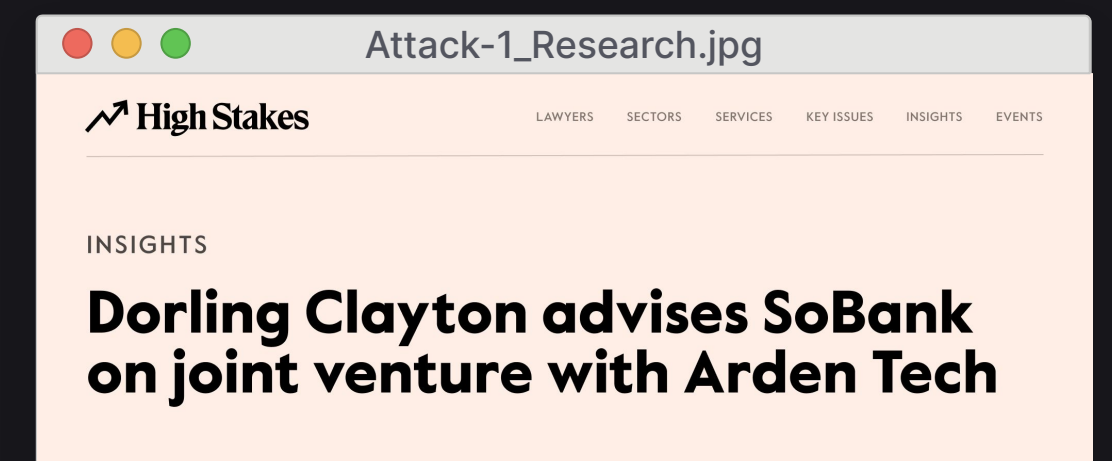
15m Reply



Liked by [redacted] a

33 MINUTES AGO

Add a comment...



High Stakes

LAWYERS SECTORS SERVICES KEY ISSUES INSIGHTS EVENTS

INSIGHTS

Dorling Clayton advises SoBank on joint venture with Arden Tech

The social network

Our digital footprints are bigger than ever¹.

There are over:

2,701,000,000 users on Facebook

1,158,000,000 users on Instagram

722,000,000 users on LinkedIn

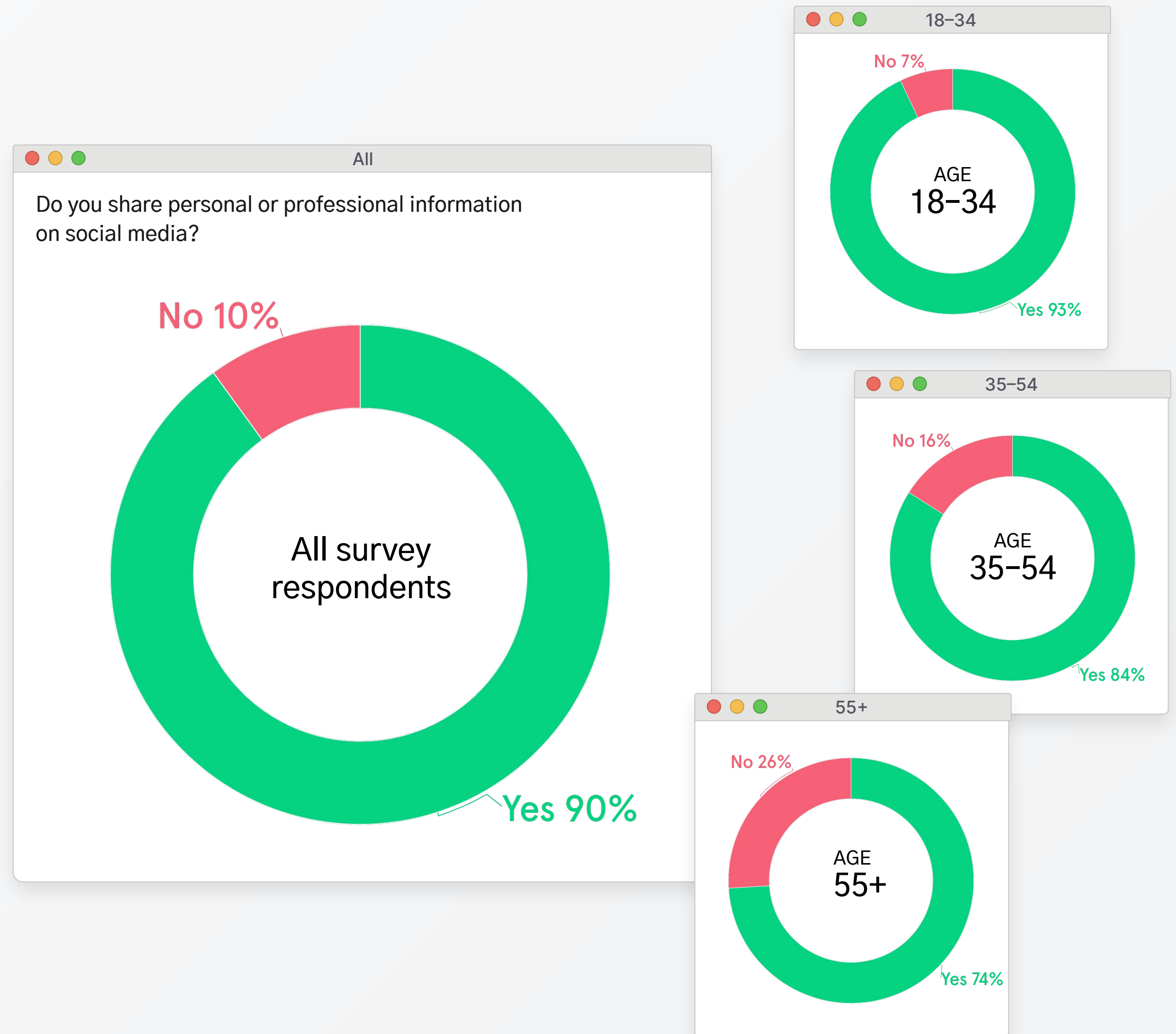
353,000,000 users on Twitter

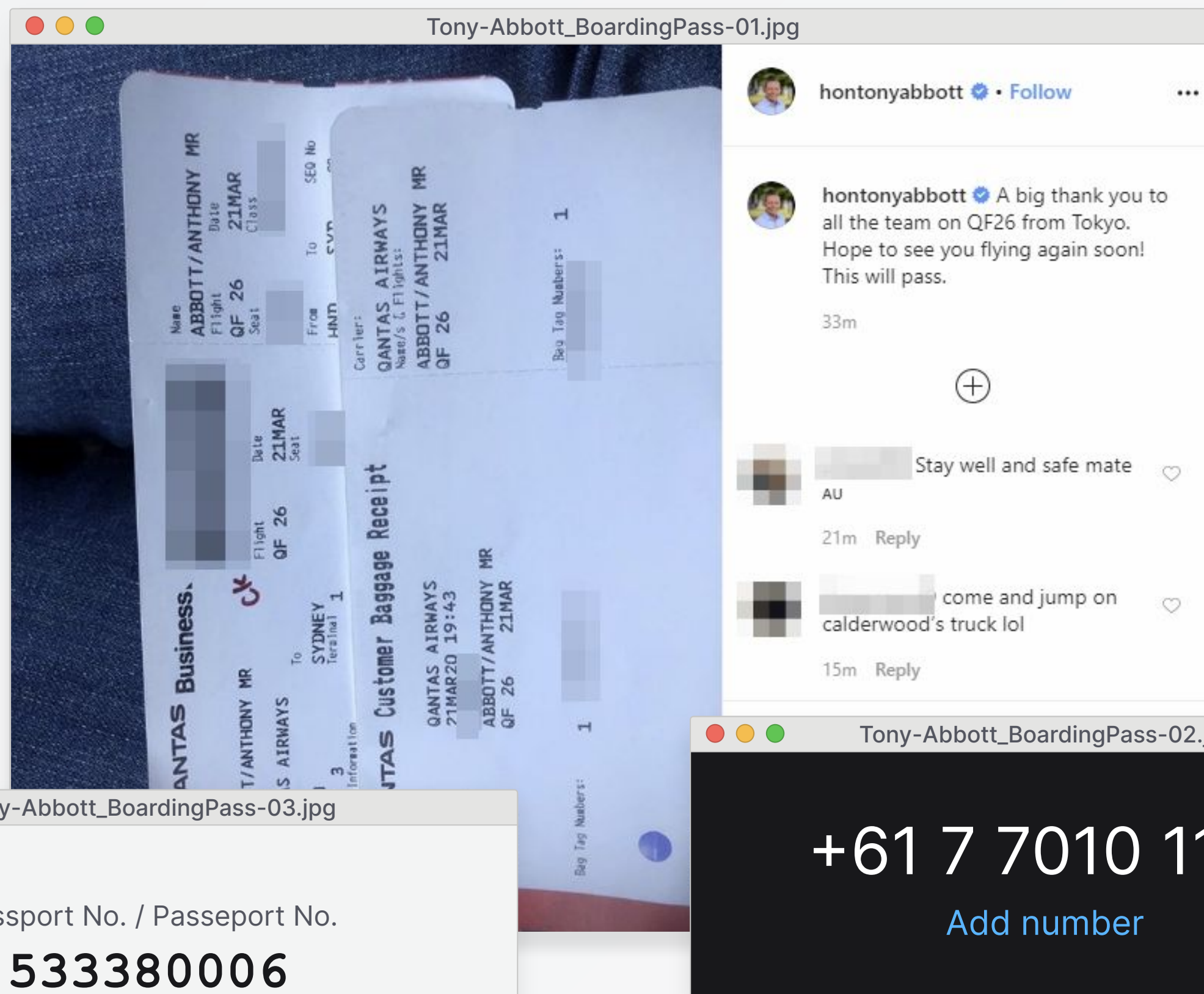
It shouldn't surprise you that 90% of people post information related to their personal and professional lives online.

This number is even *higher* among 18-34 year olds, according to our survey results. And, across LinkedIn, Instagram, and Facebook, 55% of people have publicly visible accounts.

When an account is public, **anyone can see the information you post online**, whether it's a photo of your boarding pass, or a birthday shout-out to a colleague.

Harmless, right? Unfortunately not.





This information is **gold dust** to hackers and makes reconnaissance impossibly easy.

Take the former Australian Prime Minister, Tony Abbott. He posted a picture of his boarding pass on Instagram². From the booking reference, hackers found his passport number and phone number – information that could have helped them gain access to other accounts, including sensitive personal and government information.

It didn't take much work. According to one of the hackers involved, "Anyone who saw that Instagram post could also have [his passport number and phone number]."

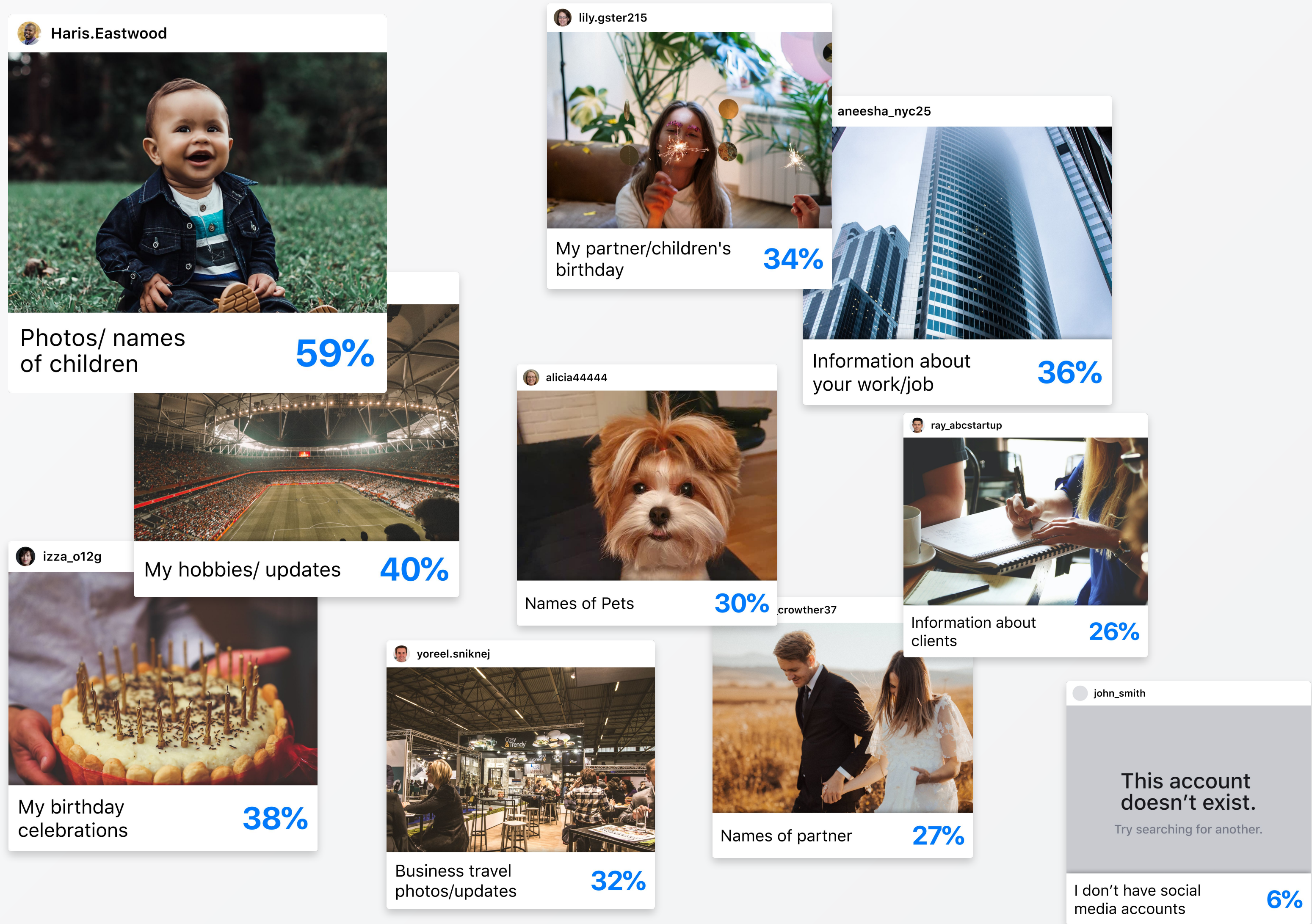
Mr. Abbott isn't the only person who posts this kind of information online...

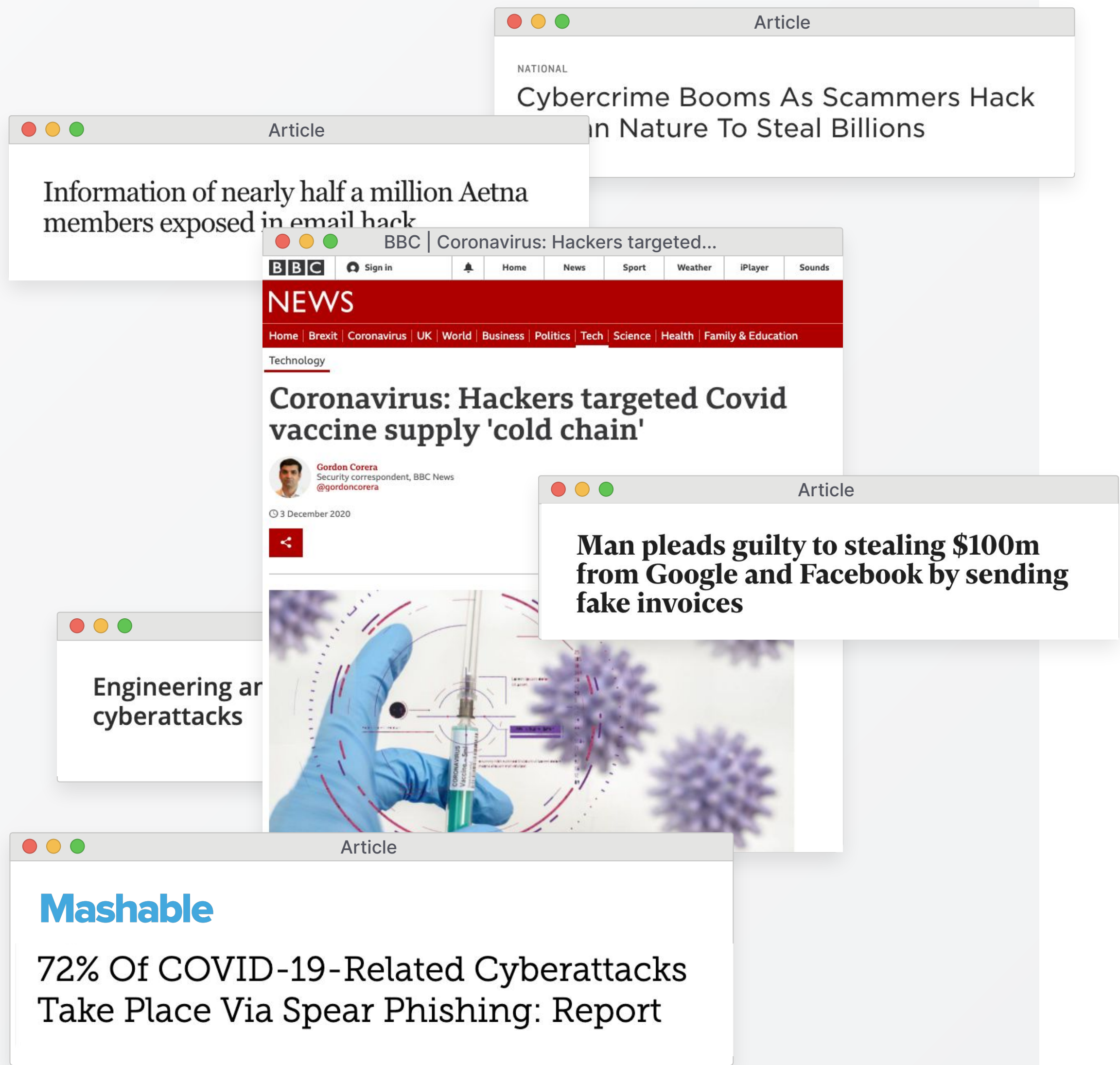
32% of employees post business travel photos and updates. Nearly 72% mention birthday celebrations. 36% share information about their jobs. And don't forget about all the information we share about our pets, partners, and children.

Hackers use all of it. Yep, even that photo of your pup.

Did you know?

JPEG files contain 'EXIF' data that can include accurate GPS locations of where the photo was taken. Many apps strip this data out before the photo goes online, **but not all.**





Hackers hack humans to hack the companies they work for

To understand exactly how hackers leverage all of this information, we have to look at a social engineering attack from start to finish.

First, a hacker identifies a target organization.

Depending on their motivations, they could choose an asset management firm with hopes of initiating a wire transfer or a pharmaceutical company with hopes of getting their hands on R&D.

From there, they'll research supply chains and vendors, study company org. charts, map employee relationships, and monitor individual behavior.

And, by running scripts, they can do this automatically and at scale.

Why do all this reconnaissance? To pinpoint potential entry points, identify viable third-parties to impersonate, and to collect information (however subtle) that'll help them nudge their targets towards unconscious (and conscious) confirmation and – eventually – trust and compliance.

“Hackers start by looking for vulnerabilities. Not necessarily exploits but vulnerabilities. Today, those vulnerabilities are people.”

 **ALON GAL**
Co-Founder & CTO, Hudson Rock

Remember

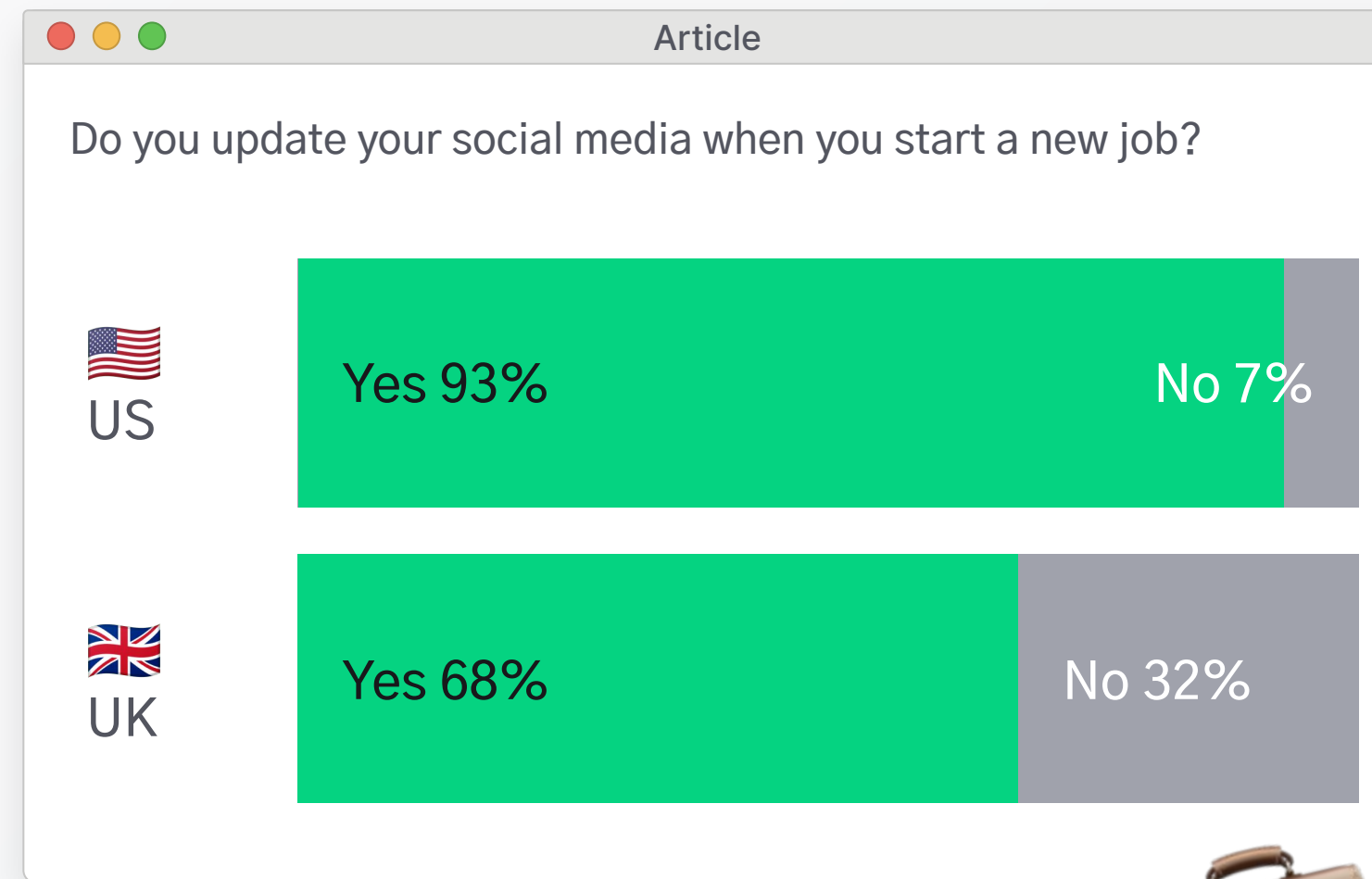
Hackers hack humans to hack the companies they work for. And a lot of the heavy lifting can be done on social media.

While behavior varies by region, most of us eagerly announce when we start a new job. In the US, almost everyone does – with 93% of employees in the US saying they update their job status on social media.

We share press releases about new clients and mergers and acquisitions. We post photos of our employee IDs and screenshots of Zoom calls. We tag our colleagues and customers in our updates and comment on theirs.

We share all of this information regularly.

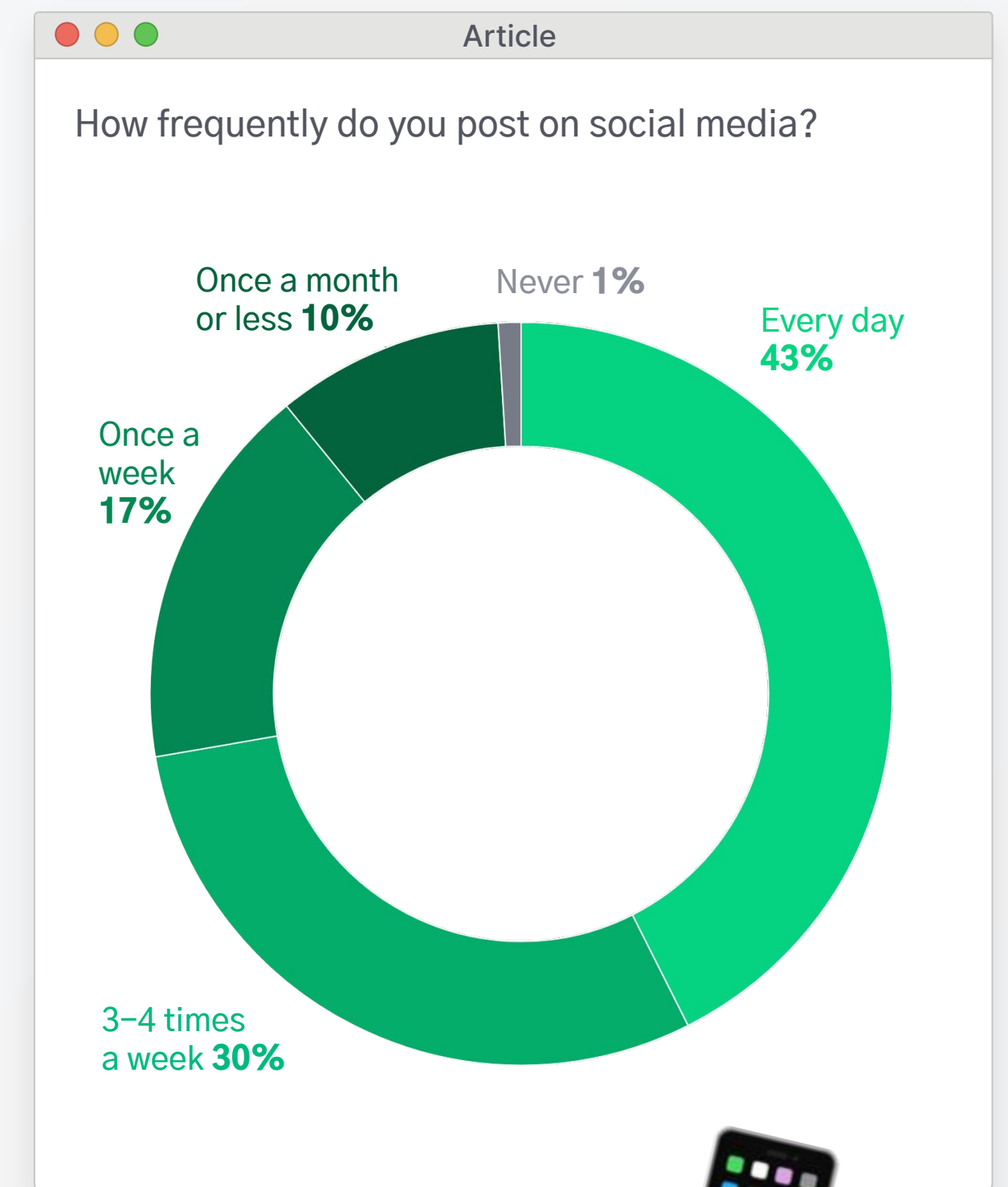
Almost half (43%) of us post every day, giving hackers up-to-date intelligence about where we're working, who we're working with, and what we're working on.



“Most people are very verbose about what they share online. **You can find virtually anything.** Even if you can't find it publicly, it's easy enough to create an account to social engineer details or get behind some sort of wall – for example, you could become a 'friend' in their circle.”



HARRY DENLEY
Security and Anti-Phishing, MyCrypto

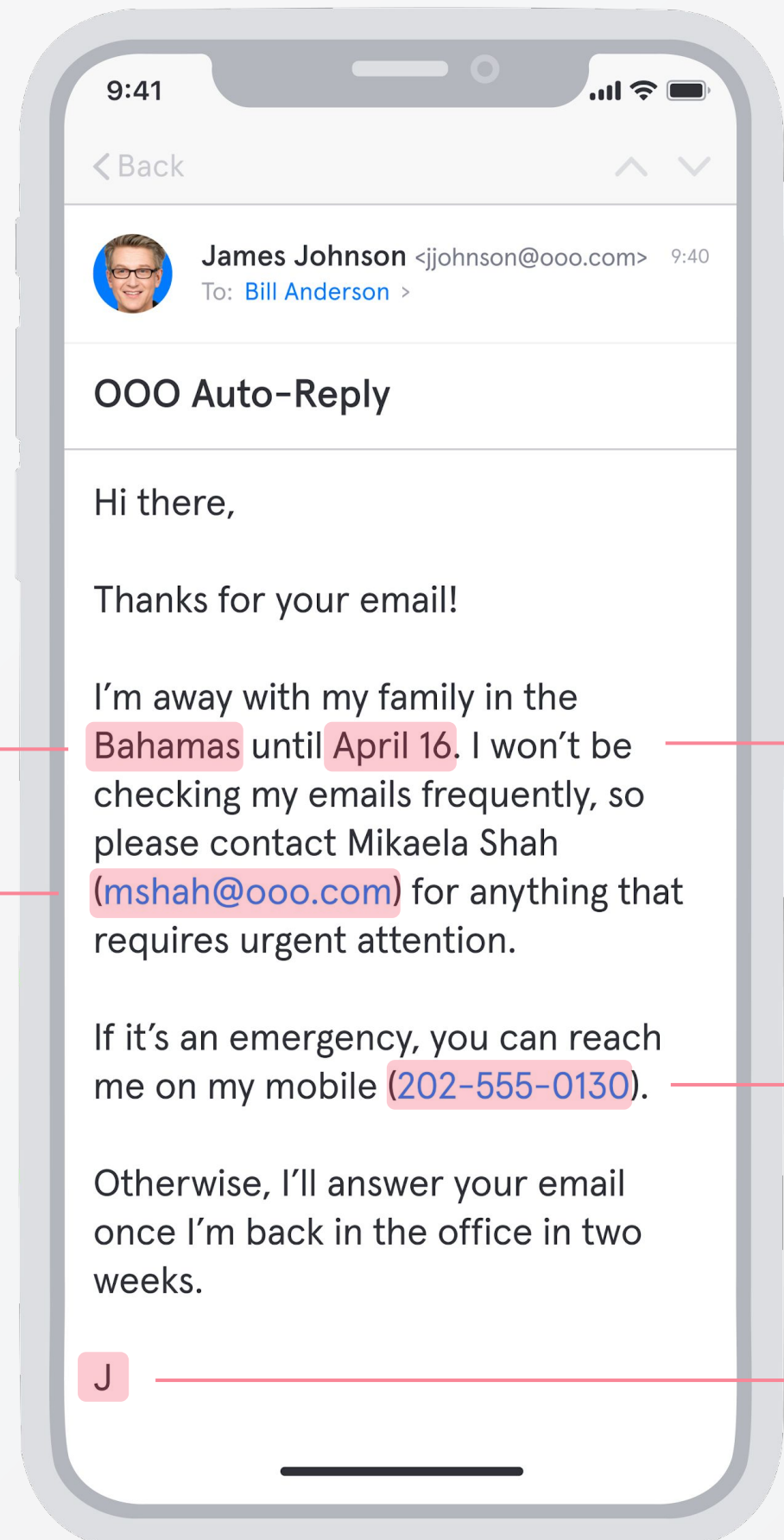


What information do you share in automated Out of Office emails?

Where you're going
43%

Point of contact
48%

N/A — I've never
set an out of office
7%



How long you'll
be out of office
53%

Personal contact
information
51%

Other information
9%

OOO? TMI*!

Our Out of Office messages – which 93% of people enable – are also filled with valuable information hackers can use to craft believable social engineering attacks.

Over half of people (53%) share how long they'll be gone while 51% offer up personal contact information. Nearly half (48%) divulge a point of contact and 43% announce where they're going.

*FYI, TMI means “too much information.”

“OOO messages—if detailed enough—can provide attackers with all the information they need to impersonate the person that's out of the office... without the attacker having to do any real work.”



KATIE PAXTON-FEAR
PhD Student, HackerOne Community

In this example of a social engineering attack, hackers use an OOO message and other publicly available information to initiate a wire transfer.

Type of Attack: **CEO/CXO Fraud**
Industry: **Financial Services**
Hacker Motivation: **(Quick) Financial Gain**

- 1 The hacker group monitors news wires for up-to-date information about banks in the United States to find their target, an asset management firm called SoBank.
- 2 They see that the company's CFO – Andrew Neal – is OOO at a conference.
- 3 Thanks to his OOO message, they're able to identify their target, Tristan Porter. They also learn that Andrew goes by "Andy" at work.
- 4 The hacker group sends a fabricated email chain that appears to be between Andy and Gregory Ellwood, Senior Partner at Dorling Clayton – SoBank's advising firm – urging Tristan to make a wire transfer.

1 **High Stakes**
INSIGHTS
Dorling Clayton advises SoBank on joint venture with Arden Tech

2 **Andrew Neal**
Chief Financial Officer at SoBank
New York City, NY
Current: Chief Financial Officer at SoBank
Jessica Thompson and Jack Worley are sharing this

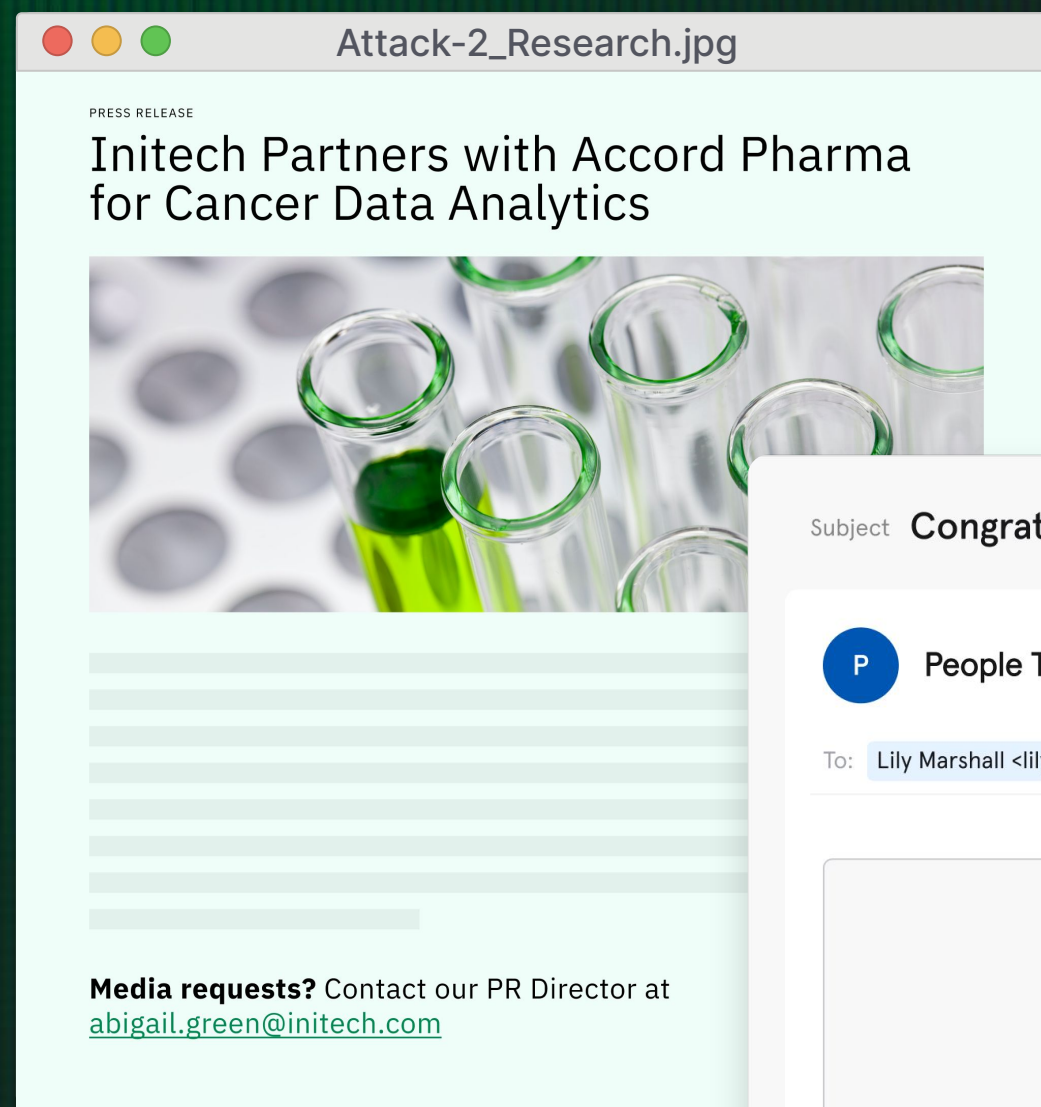
3 **Andrew Neal · 1st**
Chief Financial Officer at SoBank
I'm so excited to be joining @CliffordTucker @TaylorMac, and so many others tomorrow for @MoneyTalks2021. See you in Boston on March 8!

4 **Andrew Neal**
Chief Financial Officer at SoBank
MoneyTalks 2021
Boston, March 8

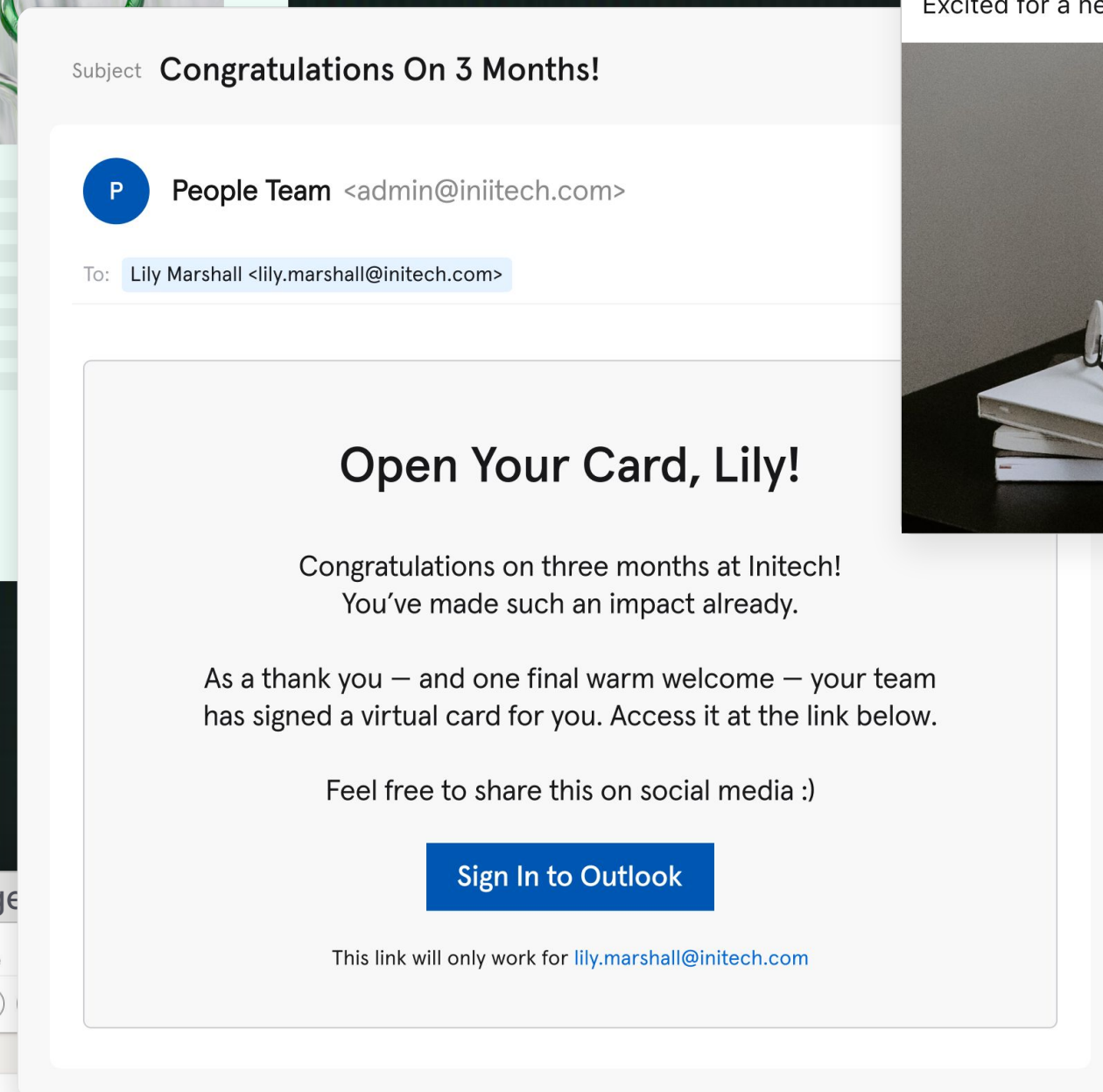
Andrew Neal
To: tristan.porter@sobank.com >
20:05
Fwd: Urgent: Acct No. Change
Hey Tristan – I know it's late but please see below thread with Gregory, Senior Partner at Dorling. Can you make this transfer to the updated acct number ASAP for me? Has to be done before the morning. Thanks and see you next week!
Andy
Sent From my iPhone
-----Forwarded message-----
From: Andrew Neal <a.neal@sobank.com>
Date: Wed, 8 March 2021 @ 19:55
Subject: Re: Urgent: Acct No. Change
To: Gregory Ellwood <gregory.ellwood@dg.com>
No problem, I'll have our Head of Accounts do it for you tonight.
On Wed, 8 March at 19:01, Gregory Ellwood <gregory.ellwood@dg.com> wrote:
Hi Andy,
Apologies for the late email on this but we updated our process for payments last week. I meant to ping you a few days ago but forgot. Can you please change the account number ASAP? I know we have something going through early tomorrow, so tonight?
Details below:

GREGORY ELLWOOD
SENIOR PARTNER
gregory.ellwood@dg.com

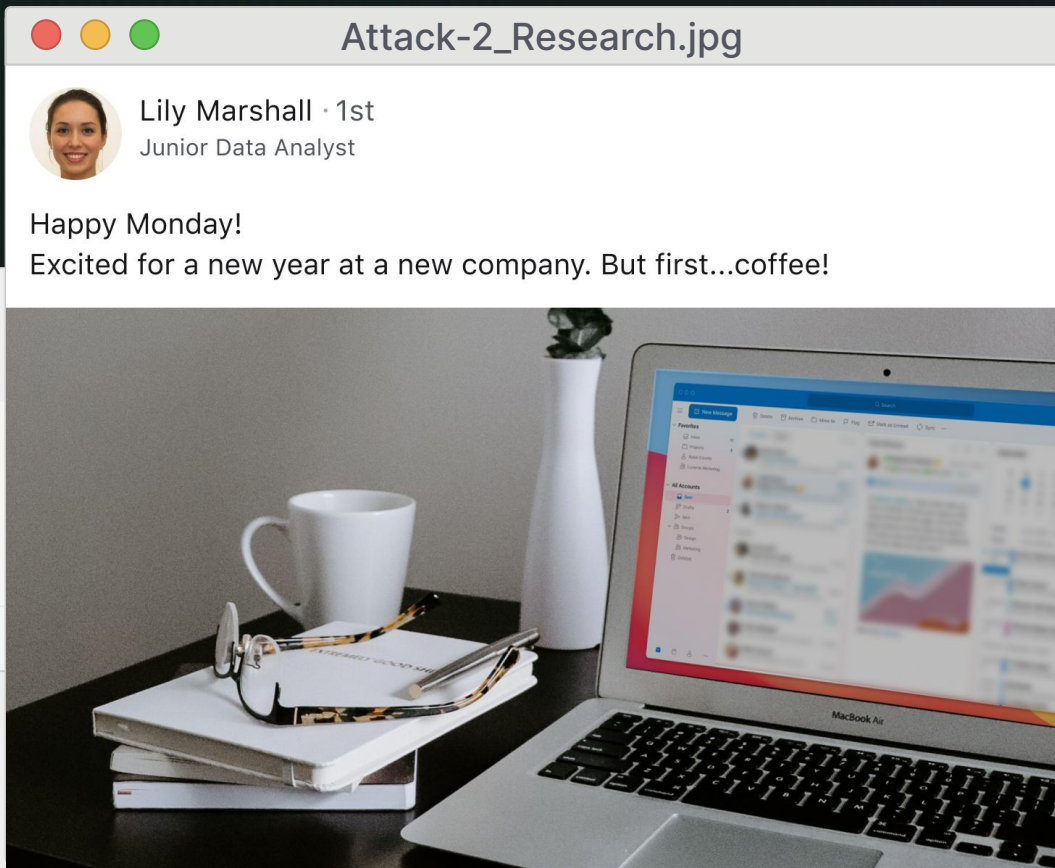
Andrew Neal
<andrew.neal@sobank.com>
OOO Auto-Reply
Thanks for your email but I'm away for the week at Money Talks. Hope to see you there!
If you need anything urgent, please contact our Head of Accounts, Tristan Porter tristan.porter@sobank.com.
Andy
Smarter Investments.
SoBank



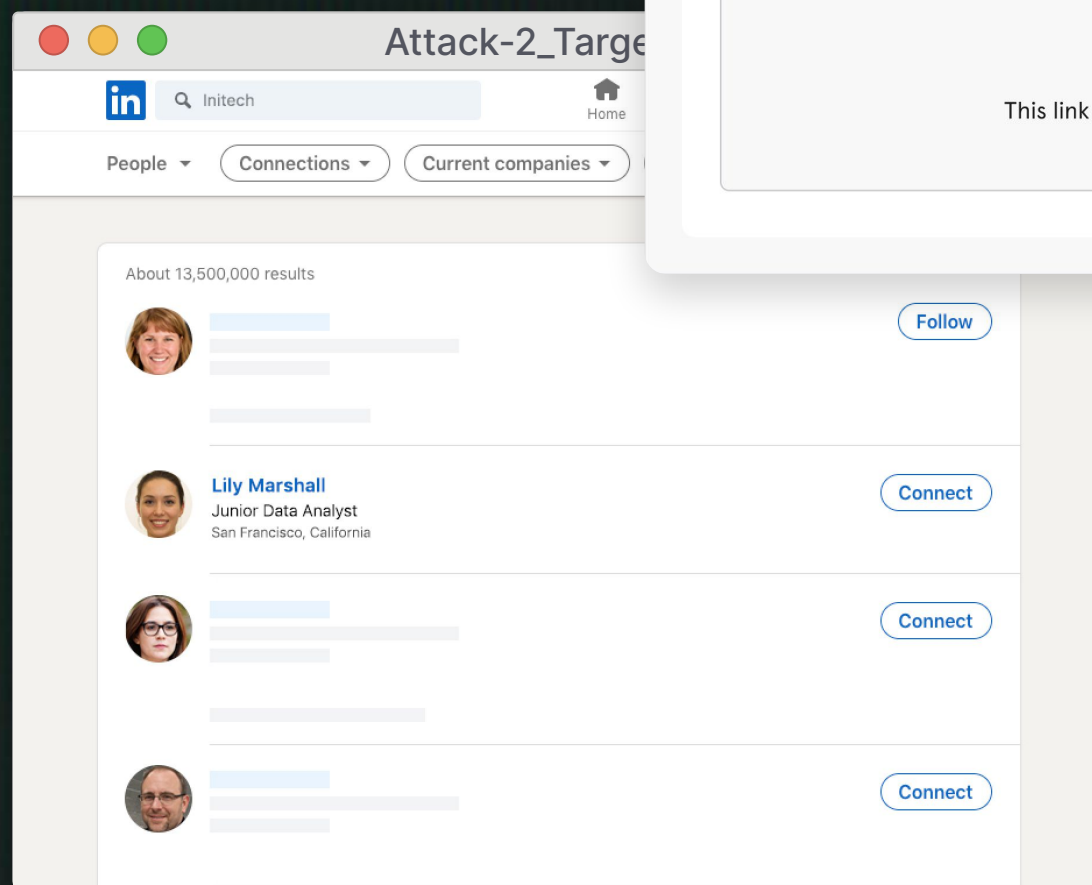
①



③



④



②

Warning:

New starters are prime targets of social engineering attacks. They're typically given their full access credentials when they start, but don't yet know who's who. They may also not have had their security training yet. Finally, given that they're new, they'll be especially keen to make a good impression.

This time, hackers leverage a trusted third-party to gain access to their target.

Type of Attack: **Account Takeover**
 Industry: **Healthcare**
 Hacker Motivation: **(Long-game) Intellectual Property**

- ① The hacker group has been monitoring news wires and eventually zeros-in on their target, Accord Pharma, a pharmaceutical company, after reading a press release.
- ② To gain access to Accord, they *first* target employees of Accord's consultancy firm, Initech.
- ③ They identify a new starter at the consultancy firm, Lily, and target her with credential phishing. The email is carefully crafted with the knowledge that the firm uses Outlook – thanks to Lily's post on LinkedIn – and leads users to a fake Outlook login page.
- ④ Lily falls for the attack, giving the hacker access to her email account
- ⑤ Once in, the hacker can email employees at the pharma company *as Lily* without raising any suspicions. That means the hacker could...
 - Embed malware into an attachment or link
 - Build rapport with employees
 - Silently gather information
 - Phish for more credentials

Not-so-strong passwords

When it comes to Business Email Compromise, information related to your professional life is important. **But your personal information can be just as valuable.**

Hackers can use information about your pets, partner, children, and even your interests to crack passwords and answer security questions, giving them full access to personal and work accounts, including password managers and even your email.

Don't believe us? 21% of people³ use information like their favorite football team, their pet's name, or birthdays when creating passwords and some of the most common security questions include:

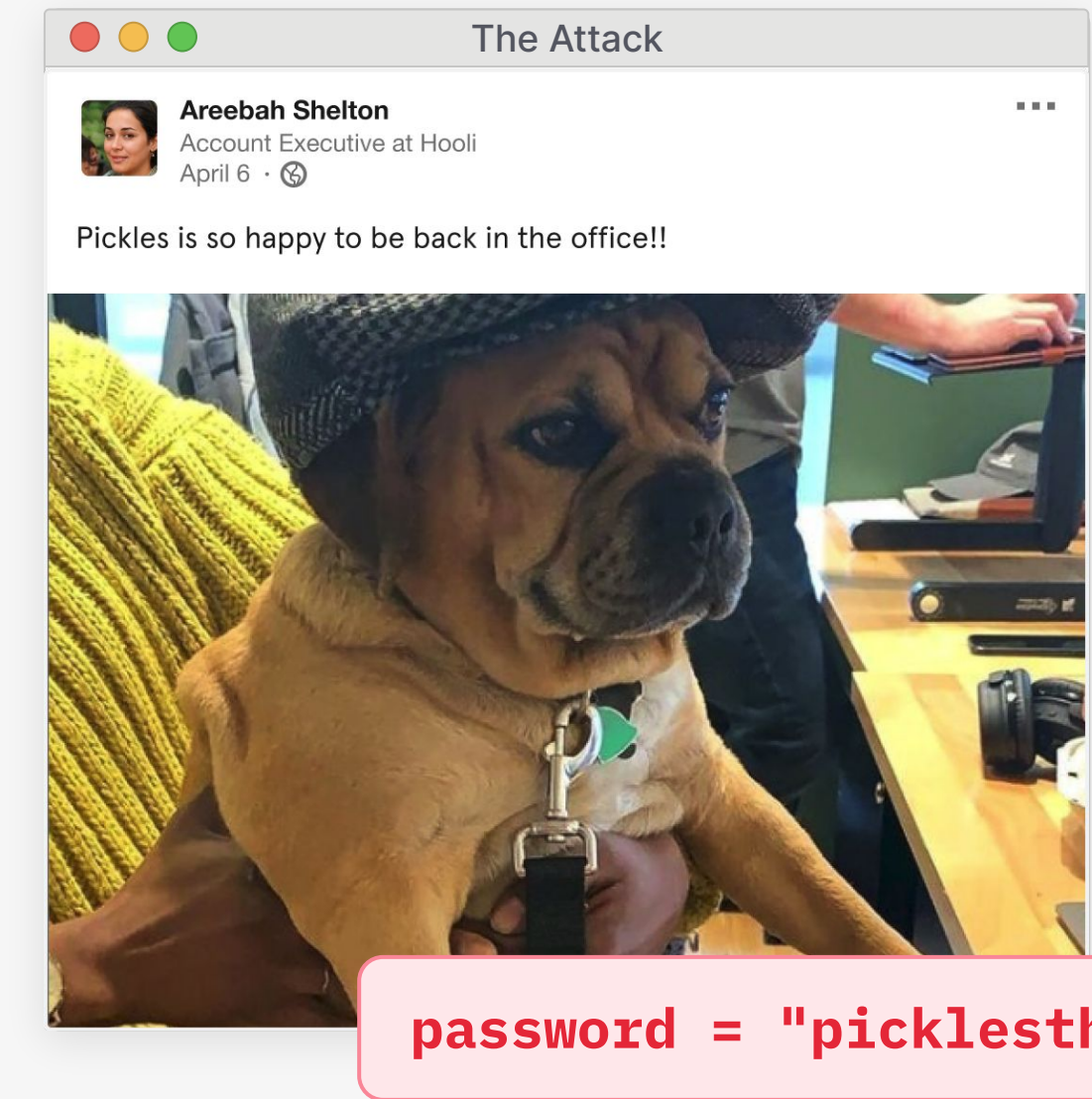
What is your mother's maiden name? What was your first car?

What elementary school did you attend?


What year were you married?

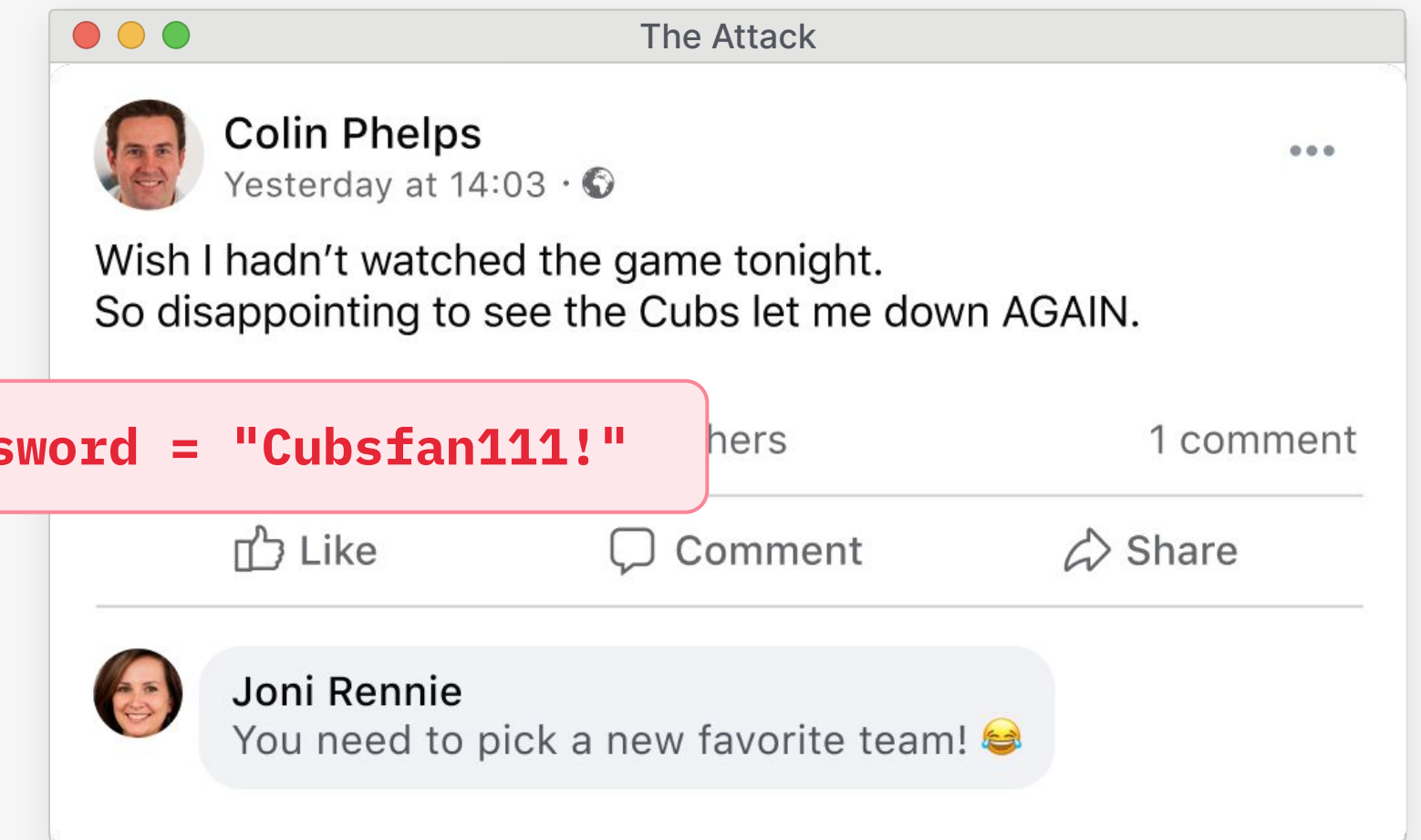
This is all readily available online. 34% of people share the names of their pets, 34% mention their children/partner, and 40% share information about their interests.

People may even unwittingly share this information via gimmicks or memes that make their rounds on social media. For example, "name generators" that ask you to combine your pet's name with your childhood street address. Sound familiar?



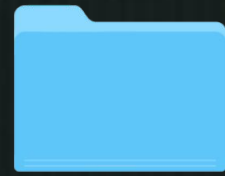
“Think about when you have to verify your identity or your account. What information do they ask you for? First name, last name, birth date. All you need is a ‘Happy Birthday!’ post on social media to garner all that information. It really is that easy.”

 [ALYSSA MILLER](#)
Hacker, Researcher, and Security Advocate

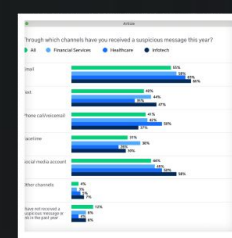


Part 2

How to level-up your email security



A hacker's toolkit.jpg



Does this look suspicious to you?.jpg

Cybersecurity Best Practice_Do's.doc

Do

Cybersecurity Best Practice_Don'ts.doc

Don't

hack.doc

HASHCAT
Hashcat

"The world's fastest password cracker." Need we say more? Oh, it's free.



We're not all security experts.jpg

alicia44444

alicia44444 Proper table manners 🍴

A hacker's toolkit

While all of this information is easy enough to find – especially if you're motivated to find it – there are plenty of tools that hackers use to connect the dots and crack passwords.


Most – if not all – of these tools were designed for the “good guys”. Penetration testers, compliance teams, and even law enforcement. In fact, some are even marketing and sales tools!

These sorts of tools are bundled together and **available for free** via Kali Linux.

“Believe me, hackers are willing to try 24/7. They have nothing but time. This is something businesses don't have. An employee working 9–5 just doesn't have the same commitment to protecting a company as a hacker has to hacking a company. That means hackers have a big advantage here.”

 **ALON GAL**
Co-Founder & CTO, Hudson Rock


Hacking-Tools.doc



Hunter.io

Designed to help sales reps, this tool allows users to find and verify employees' email addresses (personal & professional) by searching the company name.


Hacking-Tools.doc



Adobe Photoshop

Let's say someone took a selfie and – in the distant background – they have their inbox open on their laptop. With photoshop, you can zoom in without necessarily losing quality.


Hacking-Tools.doc



Sherlock

This command line tool allows anyone to “hunt down” social media accounts across social networks. If you plugged in a person's username for Instagram, for example, Sherlock would surface all other social media accounts that person has.


Hacking-Tools.doc



Google Street View

“What's the first line of your address?” is a very common security question. With Google Street View, a motivated hacker could find out exactly where you live based on a photo you took in your front yard at your gender reveal party.

Hacking-Tools.doc



Snusbase

Snusbase — a data breach search engine — was designed to help security and compliance teams prevent [account takeover \(ATO\)](#). But, it's also used by bad actors to find hacked data like email addresses, user names, and passwords.

hack.doc



Hashcat

“The world's fastest password cracker.” Need we say more? Oh, it's free.


hack.doc



Creepy

Creepy is a geolocation tool that allows you to locate a person (quite precisely) based on their social media accounts.


Hacking-Tools.doc



theHarvester

Developed using Python, theHarvester takes the hard work out of social engineering by pulling employee names and email addresses *and* company sub-domains and hosts from public sources like search engines.

Hacking-Tools.doc



HTTrack

Let's say a hacker wants to impersonate O365 to get a target's log-in details. They have to create a login page that looks like the real thing. With HTTrack, they can simply clone the real website and host it on their own server.

Hacking-Tools.doc



Maltego

Maltego is a favorite amongst security researchers. It allows users to take one piece of information (like a company name), to find another piece of information (like an employee's email address), to find *another* piece of information (like that employee's social media accounts), and so on. Bonus: It displays all of this information beautifully, in easy-to-digest graphs.

We're not all security experts

The problem isn't just that we share a lot of information online. It's also the fact that, well... security isn't top of mind for most people.

According to our survey, **only 15% of employees don't reuse passwords.**

And, while 64% of employees *do* have multi-factor authentication in place at work, hackers can (and do) work around these authentication mechanisms.

Most of us might shrug off a weak (or re-used) password, but it's big business for hackers. A recent example? **Hackers gained unauthorized access to SolarWinds by guessing passwords.**⁴

But guessing passwords isn't the only way hackers can gain access to an account. Credentials are the #1 type of data⁵ comprised in phishing attacks, most often delivered via email.

Article

Do you use the same password for multiple accounts?

Yes 76% No 15% Prefer not to say 9%

Alfiepuppy_2012 alfiepup1 alfiepuppy_2012

alfiepup1 alfiepuppy_2012 Alfiepuppy_2012

sn00pdoggyd0G alfiepuppy_2012 alfie@2012

Alfiepuppy_2012 alfiepup1 alfiepuppy_2012

alfie@2012 Alfiepuppy_2012 alfiepuppy2012

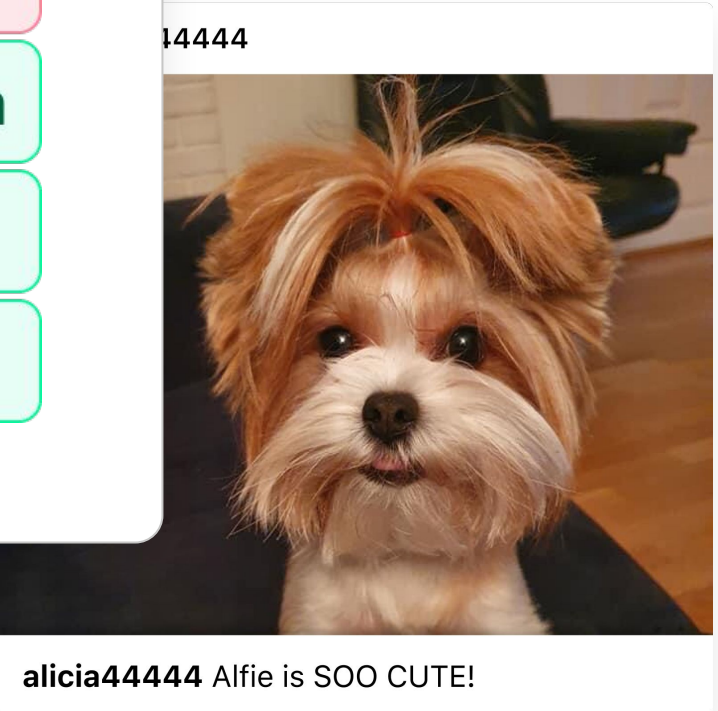
alfiepuppy_2012 alfie@2012 sn00pdoggyd0G

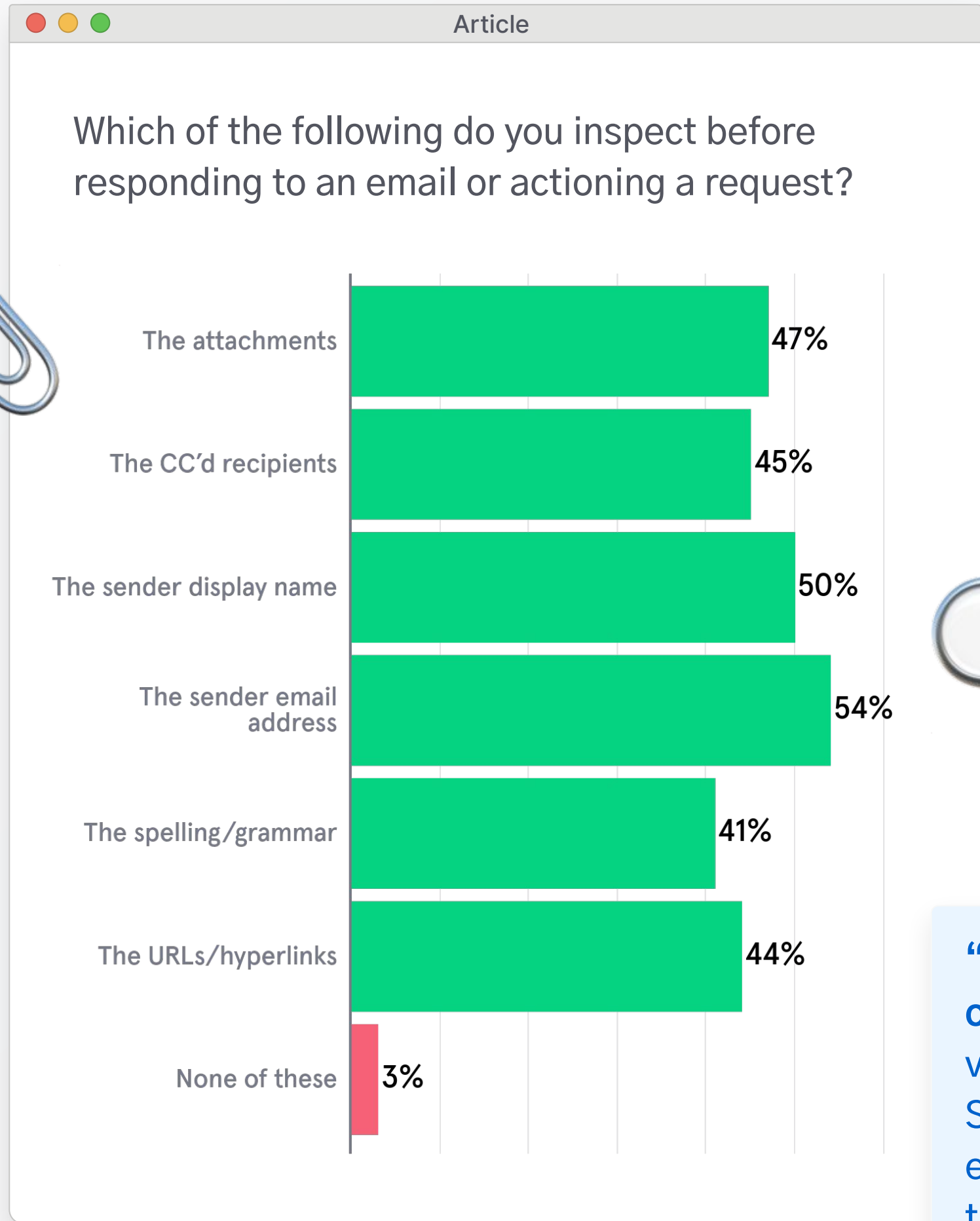
Alfiepuppy_2012 alfiepuppy_2012 alfiepup1

alfiepuppy_2012 alfieno1 WsjX01k5Wz32P@h


***** ***** YwsC6r8W^^)#Rhg]21H

***** Xrdpupb&=yz x8*2=eu6ZB





“Hackers are very strategic in the timing of their social engineering attacks. It’s very similar to marketing. Mailchimp and SendGrid publish reports about the most effective times of day to send emails... the same rules apply for phishing.”

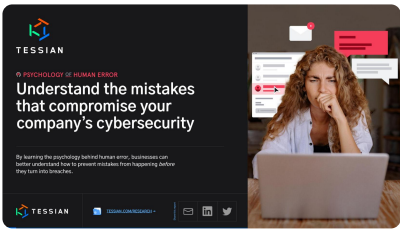
 [CRAIG HAYS](#)
Ethical Hacker

At work, just 54% of people report paying attention to the sender’s email address and less than half check the legitimacy of links (44%) and attachments (47%) before responding or actioning a request.

And, as several ethical hackers pointed out, people are even less likely to exercise caution when replying on a mobile phone or during out-of-office hours, making it easier for hackers to dupe their targets.

And this doesn’t even account for stress, fatigue, distractions, or the pressure employees are under with quick-to-click cultures.

That means even unsophisticated phishing attacks might fool the average person. In that case, what chance do we have against highly targeted and carefully crafted social engineering attacks?



You can read more about the **Psychology of Human Error** in this report →

Does this look suspicious to you?

You *could* make the argument that people don't carefully inspect their incoming emails because they're most likely not being targeted by phishing or social engineering attacks. They have no need to be diligent.

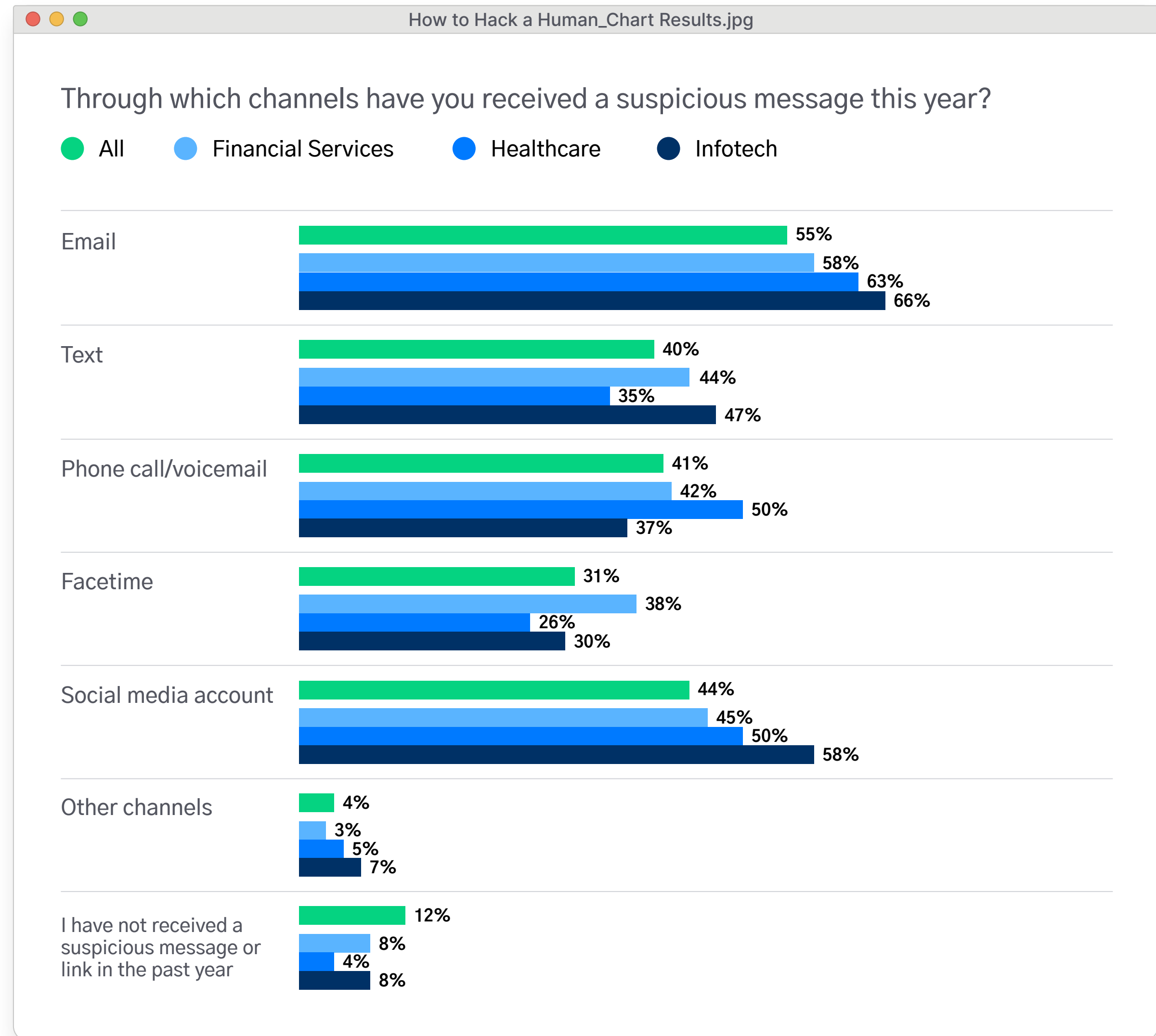
Our data tells a different story.

88% of people have received a suspicious message or link in the last year. Via which channel? Most often email, followed by social media, then text message.

And some industries are receiving more suspicious messages than others. Unsurprisingly, it's those that handle the most sensitive information that are targeted most frequently.

96% of employees working in Healthcare say they received a suspicious message in 2020. 92% of employees in both Financial Services and Information Technology say the same. **Across the board, email is the #1 threat vector.**


This begs an important question: **What are organizations doing to prevent the problem?**



Many organizations rely on training to prevent social engineering attacks like CEO Fraud, Account Takeover, and Business Email Compromise. And educating employees is an incredibly important first step.

Here's a list of do's and don'ts when it comes to managing your digital footprint, following cybersecurity best practice, and spotting advanced impersonations attacks.

“For the most part, you can't stop employees from sharing information online. You also can't stop employees from clicking on links or attachments. That's the problem! It only takes one late night for someone to make a mistake. It happens to the best of us. That means it really comes down to getting them to care about the culture of security.”

 **DAWN ISABEL**
Mobile Security Research Engineer at
NowSecure, HackerOne Community

Cybersecurity Best Practice_Do's.doc

Do

- Review your privacy settings on all your social media profiles. Be aware that some will share your information *beyond* the platform.
- Configure your OOO settings so that your message is only sent to contacts or email addresses from *within your organization*.
- Use strong passwords that don't include your name, birth date, pet's name, or other information that's easy to find online. Better yet, use a password manager like 1Password to randomly generate impossible-to-hack passwords.
- Enable 2FA or MFA.
- When reading emails, check that the sender's display name and email address match, *especially* if you're on your mobile.
- Follow in-house security policies around payment verification before actioning any requests made via email.
- Hover over links before clicking on them. If the URL looks suspicious, don't click.
- Report anything suspicious! Your security team is there to help.

Cybersecurity Best Practice_Don'ts.doc

Don't

- Re-use passwords for professional **or personal accounts**.
- Include too much information in an OOO message. The date of your return is sufficient for anyone outside of your organization. Want to be proactive? **Email customers/clients directly before you log off with relevant contact details for you or a colleague.**
- Open attachments or links from senders you don't recognize.
- Post photos of your employee ID *or* screenshots of your laptop with work "stuff" visible. For example, your email, your desktop, Zoom Meeting IDs, browser bookmarks etc.
- Be afraid to ask for a second opinion about a suspicious message.
- Assume that phishing emails are poorly crafted or riddled with grammatical errors. Remember, these are sophisticated attacks designed to look exactly like the real thing.

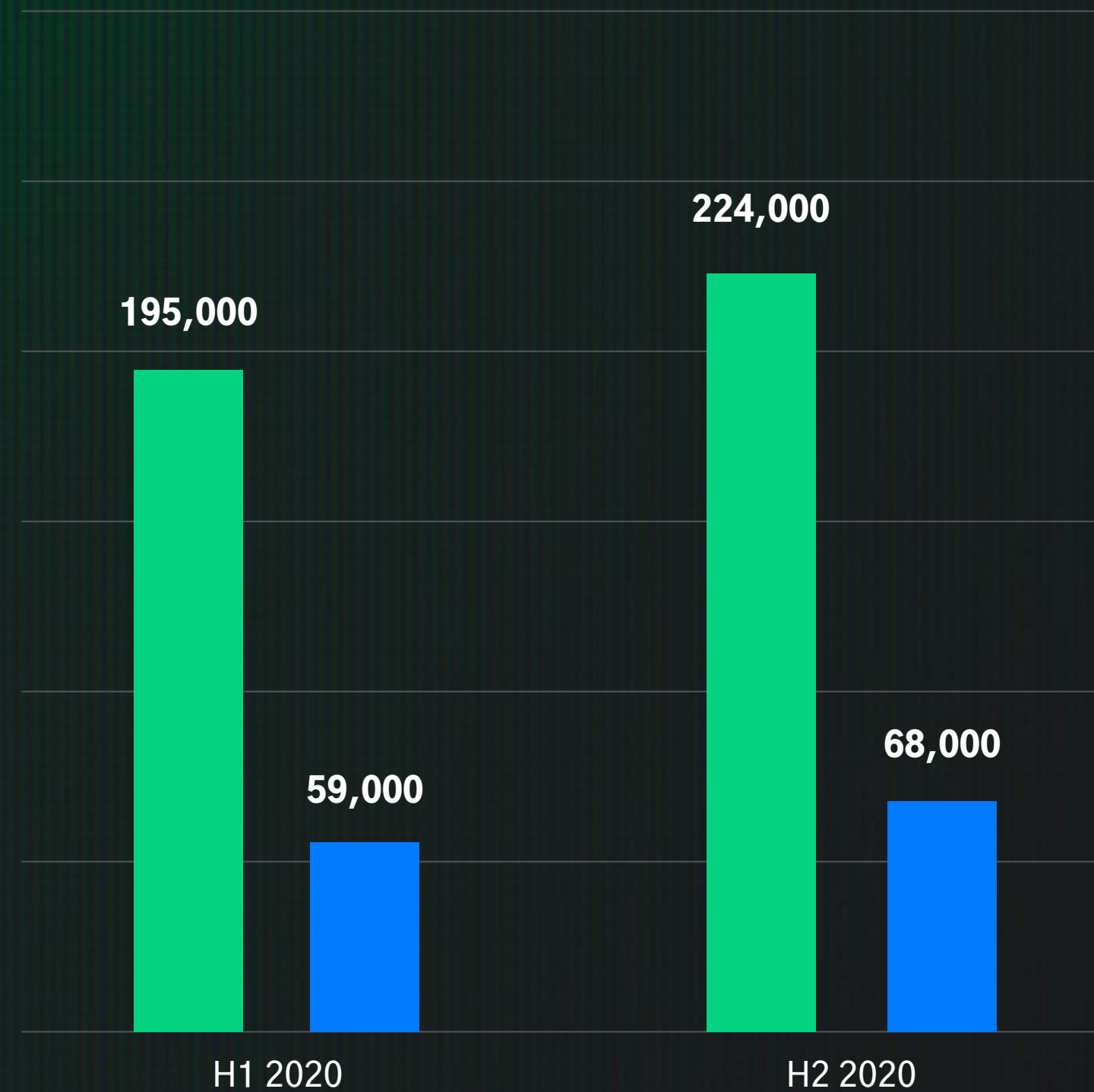
Spread the word!

Download this list of do's and don'ts to share with employees.

[DOWNLOAD NOW →](#)

Throughout 2020, Tessian Defender prevented nearly 420,000 social engineering attacks and over 125,000 attempts of wire fraud. And, we've seen a 15% increase in the number of attacks from the first half of the year to second. These are emails that slipped right past legacy solutions and native controls.


● Social Engineering Attacks ● Wire Fraud Attacks




But employees should never be the last line of defense. That's why most organizations invest in inbound email security solutions.

Unfortunately, spam filters and Secure Email Gateways just aren't enough to prevent social engineering attacks. Why? Because these outdated solutions lack the intelligent technology needed to detect the nuanced differences between a "real" email and an expertly-crafted fake one.

"We don't hire people to be spam filters or phishing email detectors. We hire them to do other jobs. The best you can do is ask them to be vigilant and educate them, but even that isn't enough. You have to put tools in place to protect them."

 [CRAIG HAYS](#)
Ethical Hacker

Tessian is different.

 **Tessian Defender** uses machine learning (ML) to protect your people from even the most advanced inbound threats.

Here's how:

- ① Tessian's machine learning algorithms analyze your company's email data, learn employees' normal communication patterns, and map their trusted email relationships — both inside and outside your organization.
- ② Tessian inspects both the content and metadata of inbound emails for any suspicious or unusual signals pointing to a potential impersonation, ATO, or BEC threat. For example, payloads, anomalous geophysical locations, IP addresses, email clients, and sending patterns.
- ③ Once it detects a threat, Tessian alerts employees that an email might be unsafe, explaining the threat in easy-to-understand language via an interactive notification.



Tessian is a leading cloud email security platform that intelligently protects organizations against advanced threats and data loss on email, while coaching people about security threats in-the-moment. Using machine learning and behavioral data science, Tessian automatically stops threats that evade legacy Secure Email Gateways, including advanced phishing attacks, business email compromise, accidental data loss and insider threats. Tessian’s intelligent approach not only strengthens email security but also builds smarter security cultures in the modern enterprise.

[TESSIAN.COM](https://tessian.com)

Methodology

In addition to using Tessian platform data, and insights garnered from interviews with the HackerOne community and experts in social engineering, we commissioned OnePoll to survey 4,000 working professionals: 2,000 in the US and 2,000 in the UK.

Survey respondents varied in age from 18–51+, occupied various roles across departments and industries, and worked within organizations ranging in size from 2–1,000+.

Publicly available third-party research was also used, with all sources listed on this page.

Midpoints and averages were used when calculating some figures and percentages may not always add up to 100% due to rounding.

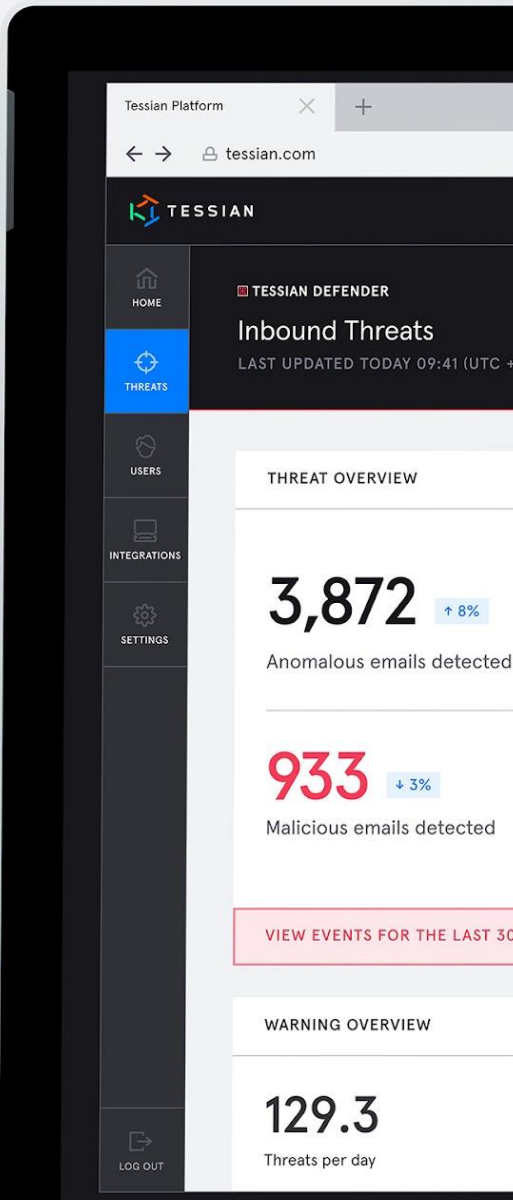
Appendix

¹ [Statista](#) ² [The BBC](#) ³ [Help Net Security](#) ⁴ [CISA](#) ⁵ [DBIR 2020](#)

About HackerOne

HackerOne empowers the world to build a safer internet. As the world’s most trusted hacker-powered security platform, HackerOne gives organizations access to the largest community of hackers on the planet. Armed with the most robust database of vulnerability trends and industry benchmarks, the hacker community mitigates cyber risk by searching, finding, and safely reporting real-world security weaknesses for organizations across all industries and attack surfaces.

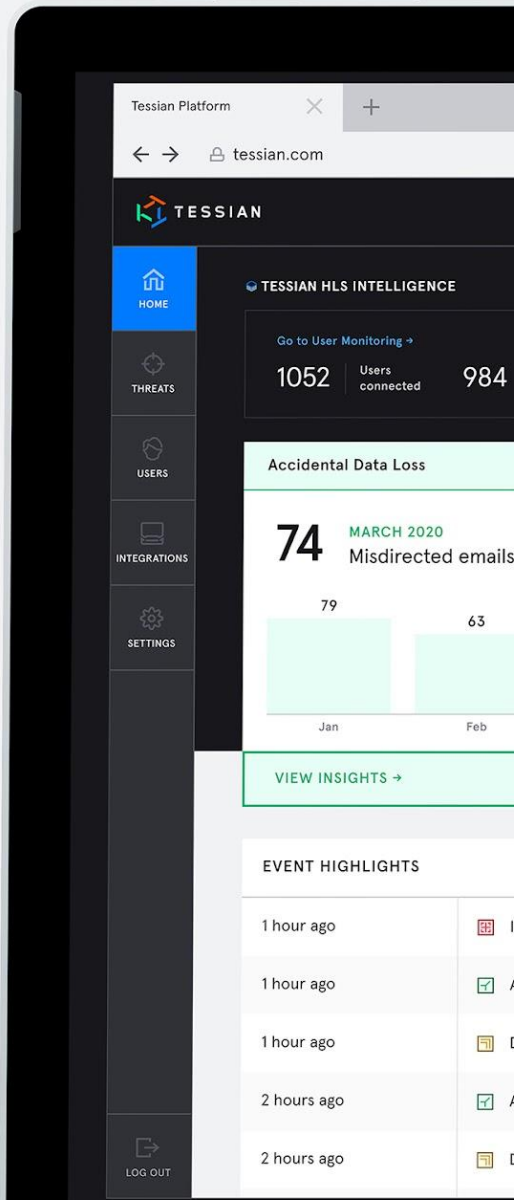
With programs designed to aid vulnerability discovery and management and products built for every stage of security maturity, HackerOne helps customers including The U.S. Department of Defense and Goldman Sachs scale security and reduce risks.



DEFENDER

Automatically prevent spear phishing, business email compromise, account takeover, and other targeted email attacks.

[LEARN MORE →](#)



HLS INTELLIGENCE

Insights and automated threat intelligence to rapidly investigate, remediate, and lower risks.

[LEARN MORE →](#)

Share this report



[TESSIAN.COM/RESEARCH](https://tessian.com/research) →