Constella

Getting Personal

The damaging impact of cybercrime on executive leadership.

2021 | Whitepaper

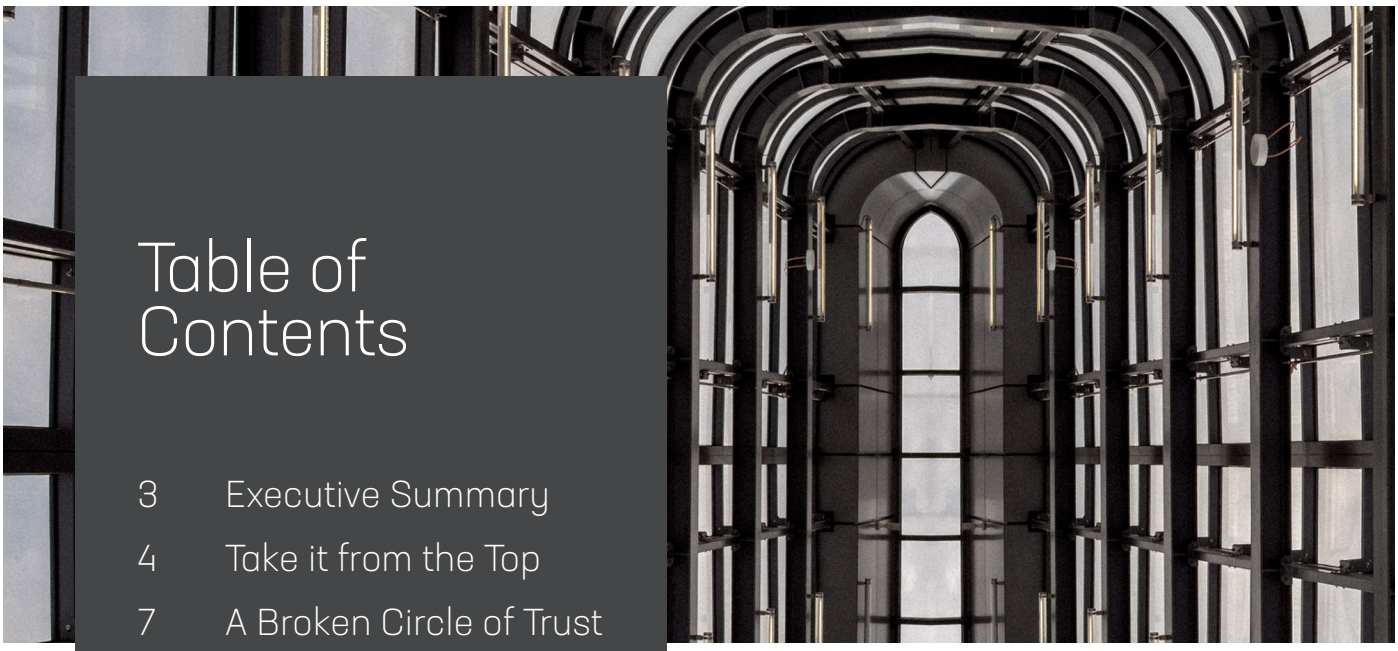


Table of Contents

Executive Summary

When it comes to cyber threats, the C-suite and board room have a lot to worry about, considering that company executives are frequent targets of cyber-attacks, with perpetrators often impersonating CEOs. Moreover, phishing attacks have increased in frequency by 667% during the Covid-19 pandemic, with threat actors utilizing more sophisticated tactics to gain access to personal, account or financial information of an employee.

- **What would a breach do to our company's reputation?**
- **What could happen to our stock price?**
- **What if our intellectual property is stolen?**
- **How could the cost of a breach affect our financials?**

These are all important questions, and smart companies consider how to answer them before an incident occurs. But there is one question that few executives think to ask until it's too late:

"What if I am the source of the breach?"

When a CEO's account is breached, it can trigger an earthquake for the entire enterprise. Aftershocks often include phishing scams, exfiltrated intellectual property, exposed stolen customer lists, and countless other incidents that can cause severe financial and reputational damage.

Constella's unique, outside-in approach can safeguard your executives, your assets, and your organization. We scour the full attack surface to uncover lost, leaked or stolen credentials and data to rapidly identify threats and mitigate risk before any damage can occur.

Take it from the Top

Increasingly, cybercriminals are targeting company leadership to gain access to networks, information, notoriety, and money. Nobody is safe. Consider just a few of many executives and high-profile individuals in the news media who suffered cyberattacks or malicious hacks recently:

Exposed Executives and Celebrities

Alf Goransson, Former CEO of Securitas

IDENTITY THEFT

Stolen identity was used for a false loan application. No legal action was taken until District Court declared him bankrupt.

Bo Shen, Founder of Fenbushi Capital

SOCIAL ENGINEERING

Bo, an early investor in digital currencies Ethereum and Augur, was considered a "whale." Hackers stole and dumped his REP and ETH, which then caused trading prices to plummet.

Barbara Corcoran, Celebrity

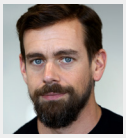
BUSINESS EMAIL COMPROMISE

Lost nearly $400,000 in a classic email fraud scam after a fraudster persuaded her book-keeper to wire funds to a new bank account.

Bill Gates, Co-Founder of Microsoft

MISINFORMATION

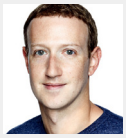
Social media users shared posts about COVID-19 vaccines and population control that falsely attributed quotes to Bill Gates.



Jack Dorsey, CEO of Twitter

ACCOUNT TAKEOVER

A stream of rogue tweets – including racial slurs – were posted to the Twitter chief executive's own Twitter account. One of the tweets posted a Twitter handle for someone who purported to take credit for the account takeover.



Mark Zuckerberg, CEO of Facebook

DATA LEAK

Mark Zuckerberg's contact details were included in the leaked records of more than 500M Facebook users.

Joe Biden, U.S. President

SOCIAL MEDIA HIJACK

Hackers gained access to more than a dozen high-profile accounts to display tweets telling followers to send bitcoin to a specific address.

Elon Musk, CEO of Telsa

SOCIAL MEDIA HIJACK

Hackers gained access to more than a dozen high-profile accounts to display tweets telling followers to send bitcoin to a specific address.

Jeff Bezos, CEO of Amazon

SOCIAL MEDIA HIJACK

Jeff Bezos' mobile phone was hacked after receiving a WhatsApp message sent from the personal account of the crown prince of Saudi Arabia. The encrypted message from the number used by Mohammed bin Salman is believed to have included a malicious file that infiltrated Bezos' phone.

These examples are of sophisticated executives at the helm of cutting-edge tech companies or people in the public eye with careers deeply tied to their reputation, yet their accounts and identity are often compromised using the same tactics that put us all at risk. Let's start with the most popular tactic by cybercriminals – phishing scams.

1. CEO Phishing Scams

Cybercriminals use phishing to gain access to identities and networks for one good reason – it works. Every single day, even the most tech-savvy execs fall for spoofed emails. By clicking on a seemingly innocuous link or entering a password in a familiar looking website, they put untold personal and corporate information and reputations at risk.

Preventing phishing scams is particularly vexing for corporate IT departments because they often do not set off spam traps. They aren't mass emails and they use familiar domains.

In 2019, the City of Ottawa's treasurer was duped in an email scam, unknowingly transferring nearly $100,000 to a phony supplier.

Ubiquiti Networks, a San Jose, CA-based maker of networking technology, was taken for $46.7 million when a hacker "impersonated" executives and directed funds to be transferred to an overseas bank.

85%
of All Organizations
Have Been Victims of Phishing Attacks.

– Intel Security Phishing Report

KrebsonSecurity
In-depth security news and investigation

Tech Firm Ubiquiti Suffers $46M Cyberheist

Networking firm Ubiquiti Networks Inc. disclosed that cyber thieves **recently stole $46.7 million** using an increasingly common scam in which crooks spoof communications from executives at the victim firm in a bid to initiate unauthorized international wire transfers.[1]

UBIQUITI NETWORKS

Earlier this year, the FBI reminded organizations of the serious threat posed by business email compromise (BEC) scams, declaring that it caused more than $1.8 billion worth of losses to businesses last year. BEC schemes frequently impersonate executives in an attempt to pressure an employee to transfer funds or confidential information.

KrebsonSecurity
In-depth security news and investigation

FBI: Business Email Compromise Cost $1.8B in 2020

The FBI's Internet Crime Complaint Center (IC3) reports the American public submitted 791,790 complaints in 2020, marking a 69% increase from 2019. **Total losses from cybercrime exceeded $4.1 billion.** Business email compromise (BEC) scams were the most expensive, with 19,369 complaints and adjusted losses of approximately $1.8 billion. Officials report BEC scams have evolved since 2013, when these attacks typically spoofed email accounts of chief executive officers or chief financial officers and requested wire payments. The scams have since evolved to compromise personal emails and vendor emails. In 2020, the IC3 saw more BEC complaints detail identity theft and funds being converted into cryptocurrency.

[1] August 8, 2015. Brian Krebs. Tech Firm Ubiquiti Suffers $46 M Cyberheist
[2] March 18, 2021. Adam Curtis. FBI: Business Email Compromise Cost $1.8B in 2020

2. Stolen Credentials

If cybercrime is a fast-moving wildfire across the global internet, stolen credentials are the oxygen. **They are the source of 80% of all data breaches.**

Unknown activists have posted nearly **25,000 email addresses and passwords** allegedly belonging to the National Institutes of Health, the World Health Organization, The Gates Foundation and other groups working to combat the coronavirus pandemic.

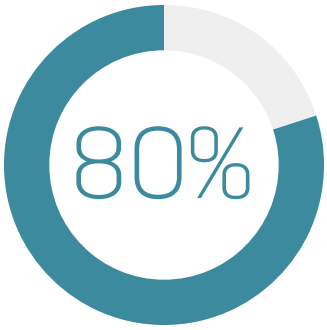
Like the rest of us, executives frequently use the same username and password combinations to log in to multiple accounts. **On average, most people use 2 - 5 passwords to access 25 accounts.**

This means that once a hacker gains the credentials that unlock one site, with a little time and the right software, he or she can gain access to the executive's other online accounts, including the enterprise network. This is an all-too-common way intellectual property, money and identities are stolen, and networks are held for ransom.

After the credentials are used, accounts drained and networks ransacked, criminals usually sell (or dump) the information on the dark web for others to use. At this point, it is a "free for all" and the stolen credentials are available for anyone. It's akin to leaving your keys in the ignition with the engine running and the doors unlocked.

Mark Zuckerberg used the same password ("dadada", seriously) to login to his Facebook, Adobe and LinkedIn accounts. Needless to say, they were breached multiple times. The last time, he learned of the breach by a tweet sent by hacker from his very own Twitter handle!

At Constella, we estimate an 80% chance that a hacker can find a password belonging to the victim if 3 different accounts are able to be tested.



92%

of executives have had their credentials exposed.

facebook

EMAILS	BREACH/SITE	PASSWORD ALGORITHM	DECRYPTED PASSWORD
mzuckerb@fas.harvard.edu	Linkedin	SHA1	dadada
mzuckerb@fas.harvard.edu	MySpace	SHA1	*****fee
mzuckerb@fas.harvard.edu	Last.fm	MD5	*****v3a
mzuckerb@fas.harvard.edu	Adobe	3DES	dadada
zuck@facebook.com	Tumblr	SHA1	*****nis
mark@facebook.com	Dropbox	SHA1	*****325
mark@facebook.com	Fling	None	*****980
mark@facebook.com	VK	None	*****123
mark@facebook.com	Adobe	3DES	dadada

Constella's recent survey of 100+ cybersecurity leaders indicate that about **1 in 4** cybersecurity leaders have used the same password for both work and personal use.

A Broken Circle of Trust

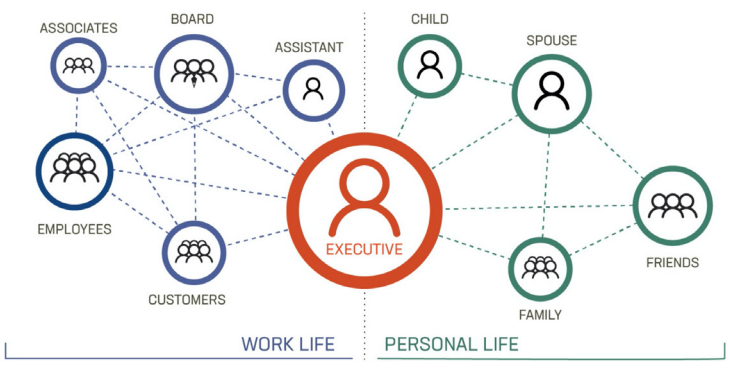
By analyzing hundreds of breaches and deconstructing how criminals have stolen identities, Constella determined that sophisticated cyber crooks monitor people close to the executive for clues about his or her vulnerabilities and possible attack vectors.

To prevent this, Constella's executive identity protection services also monitor the identities in a leader's circle of trust, including spouses, children, close friends, assistants and others. In addition to more traditional methods, this protective bubble may be the best way available today to prevent a high value target and his or her circle of trust from being breached.

For companies though, there isn't any tactic or set of tactics they can adopt to thwart cyber criminals. It takes a fundamentally different way of looking at cybercrime. It is a business risk, so building in safeguards and advanced monitoring into everyday operations is a necessity. Or cybercrime will be an inevitability.

Protect the Attack Surface

Protection from all the pieces of information from the closer Circle of Trust of the Executive.



PASSWORD SECURITY CHECKLIST

- ✓ Use a unique password for every site, or try using a password manager like 1Password or LastPass.
- ✓ Keep contact and recovery information updated.
- ✓ Turn on two-factor authentication. Be wary, adding your cell phone number can make it less secure if someone knows or can access your phone number.
- ✓ If a service only supports two-factor authentication via text message, then contact your phone company to put a password or PIN on your account that's not your social security number.
- ✓ Check the list of apps and delete ones you do not need.

Accidents Happen

Notwithstanding all of the attention lately on careful information security practices, hundreds of millions of files are exposed annually just by accident.

Perhaps the best (or worst) example of this occurred when a contractor for the Republican National Committee left detailed information on 200 million voters open -- by mistake -- to anyone who entered the Amazon subdomain "dra-dw." The repository of 1.1 TB of data was not password protected and left open to download.

Personal Details of Nearly 200 Million US Citizens Exposed.

Sensitive personal details relating to almost 200 Million US citizens have been accidentally exposed by a marketing firm contracted by the Republican National Committee. The 1.1 terabytes of data includes birth dates, home addresses, telephone numbers and political views of nearly 62% of the entire US population.[3]

You can bet that voter data is in the hands of hackers. Also in the hands of hackers: security journalist Brian Krebs first reported the discovery of more than 885 million sensitive documents exposed online by insurance giant First American Financial. Those files stored on the company's website contained bank account numbers, bank statements, Social Security numbers and more. All of that sensitive information, which dated back to 2003, was available without any protection and could be easily accessed.

First American Financial Corp. Leaked Hundreds of Millions of Title Insurance Records.

The website for Fortune 500 real estate title insurance giant First American Financial Corp. leaked hundreds of millions of documents related to mortgage deals going back to 2003. The digitized records – including bank account numbers and statements, mortgage and tax records, Social Security numbers, wire transaction receipts, and drivers license images – were available without authentication to anyone with a Web browser.[4]

Equifax to Pay $575 Million as Part of Settlement with FTC, CFPB, and States Related to 2017 Data Breach.

Equifax Inc. agreed to pay at least $575 million, and potentially up to $700 million, as part of a global settlement with the Federal Trade Commission (FTC), the Consumer Financial Protection Bureau (CFPB), and 50 U.S. states and territories, which alleged that the credit reporting company's failure to take reasonable steps to secure its network led to a data breach in 2017 that affected approximately 147 million people.[5]

[3] BBC News. June 19, 2017. Personal details of nearly 200 million US citizens exposed

[4] May 24, 2019. Adam Curtis. First American Financial Corp. Leaked Hundreds of Millions of Title Insurance Record

[5] July 22, 2019. Adam Curtis. Equifax to Pay $575 Million as Part of Settlement with FTC, CFPB, and States Related to 2017 Data Breach

Sent Packing

CEOs are learning that cyber risk goes well beyond their personal brand or bank account. It can impact their very livelihood. The list of CEOs and other senior executives who have been fired in part or entirely due to a cyber breach is long and growing. C-suite officials at Target, Home Depot and Sony were all sacked, for example. Ashley Madison's CEO was also forced out, albeit after the site's third leak.

The harsh consequences stem from the fact that CEOs have a fiduciary responsibility to take every reasonable step to protect a company's data, intellectual property, reputation, customer lists and other assets. Shareholders, regulators and consumers demand accountability.

Under what is known as the Caremark Standard, board members may be held personally liable if they fail to ensure reasonable internal controls are in place and adequately oversee risk.

Government officials face the same consequences. Senior administration officials from Utah, Texas, Arizona and other states have all lost their jobs as a result of cyber breaches.

"The FBI estimates that organizations victimized by CEO fraud attacks lose on average between $25,000 and $75,000. But some CEO fraud incidents over the past year have cost victim companies millions – if not tens of millions – of dollars."

– Brian Krebs, Cybersecurity Expert

Spare Me

So how can a corporate leader, celebrity, sports star or other high-profile person reduce the likelihood of having their identity compromised? How can they avoid inadvertently allowing the organization they lead to be hacked?

It's frightening but true: There are no guarantees. But there are steps you can take to reduce the likelihood of being a victim or unwitting accomplice to a cybercrime. For example, update software on all devices; install anti-virus, personal firewall software; use complex passwords, change them often and don't reuse them across sensitive accounts.

Further, employers should train employees on how to avoid phishing scams and conduct random tests. The FBI recommends businesses use two-factor authentication wherever possible, and verify significant transactions with an old fashioned phone call.

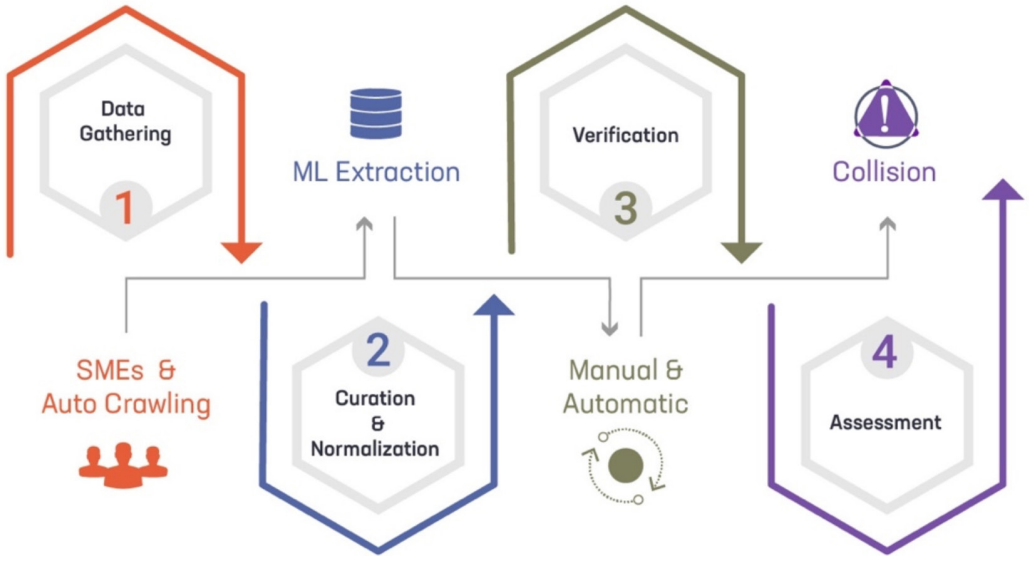
However, to provide an additional layer of protection, Constella offers executive protection services which alerts high risk targets immediately after their credentials or personal information appear on the dark web to mitigate risks and emerging threats before any damage can occur.

Constella scours the surface, social, deep and dark Web detecting exposed credentials and stolen data. Subject matter experts and automated crawlers monitor, analyze, authenticate and attribute breached data from the Darknet and underground communities. And generate real-time alerts when breached data is discovered.

This approach provides executives the opportunity to change their username and password combinations, update accounts, freeze credit or contact necessary firms in order to contain or prevent theft and mitigate risk from the exposed information.

20+ Subject Matter Experts (SMEs) and Automatic Processing

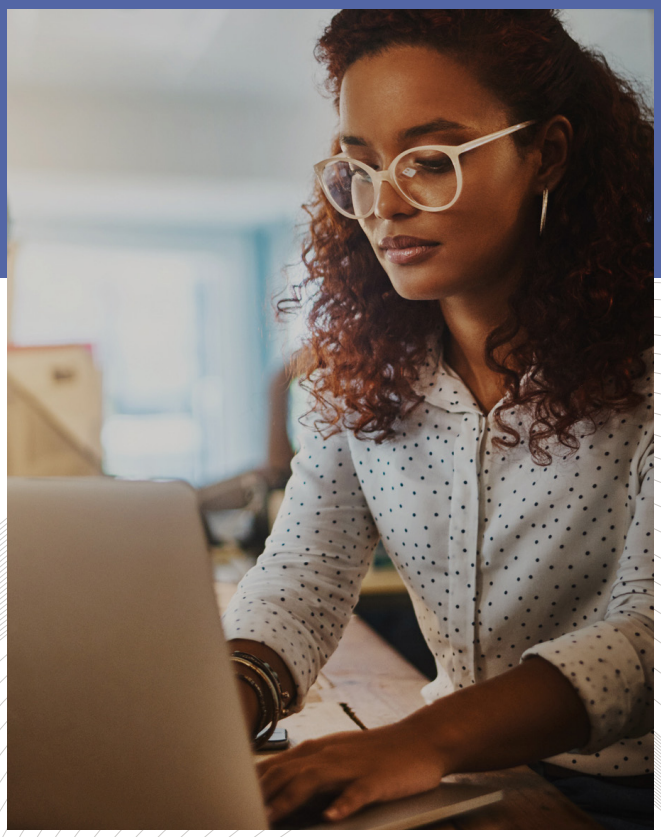
Constella curation and verification process.



Today, companies and executives themselves need to be more proactive. This involves active monitoring on the dark web, alerting executives as soon as their credentials have been stolen, and preventing network access when credentials have been compromised in other breaches.

> The FBI estimates that organizations victimized by CEO fraud attacks lose on average between $25,000 and $75,000. But some CEO fraud incidents over the past year have cost victim companies millions – if not tens of millions – of dollars."

- Brian Krebs, Cybersecurity Expert



Conclusion

Faced with personal, professional and corporate risk, what is a CEO to do? The palace wall approach – building defenses, such as firewalls, with the hope that nobody breaks in -- is no longer enough. If your credentials are not already exposed, it's just a matter of time before they are.

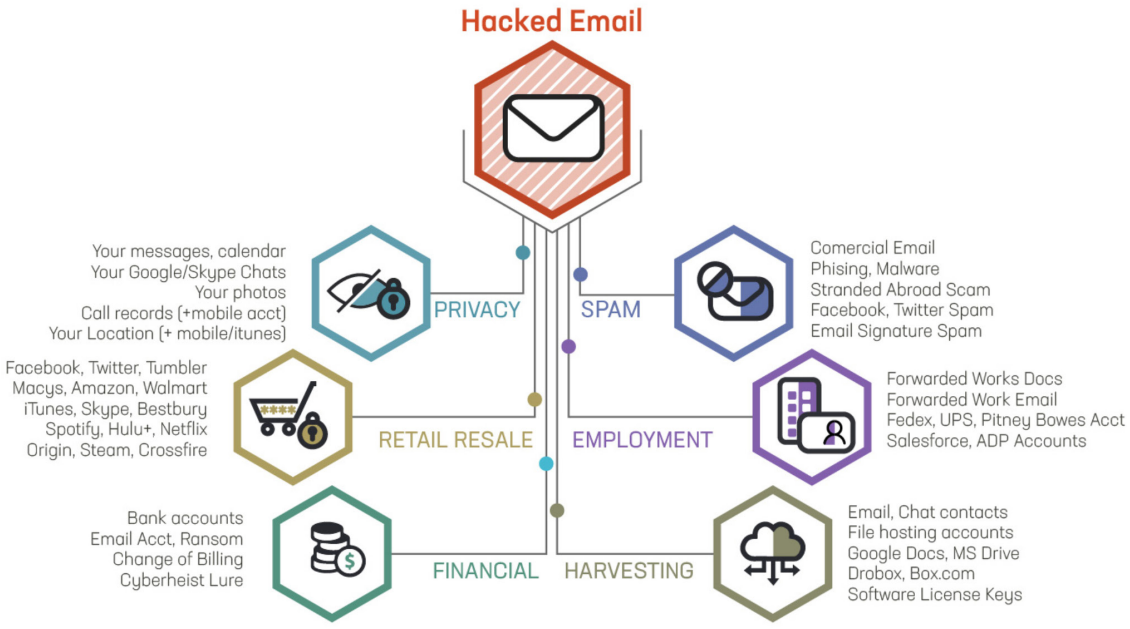
More than 5 Billion personal records were leaked in Q1 of 2021.

atlasVPN

Aside from the obvious, sensitive accounts you need to monitor and safeguard such as your banking, insurance, healthcare, credit unions, shopping, a breach to your email will give access to more than you are probably aware.

Email accounts are a single source of personal information that you can't afford to let out. Cyber criminals can use your life events against you by reading your email, having a baby, getting married or divorced, accepting a new job offer, opening a new credit card, filing your taxes, etc. Not to mention, your email provides access to many of your accounts with even more rich data about you.

Value of a Hacked Email Account



About Constella Intelligence

Constella Intelligence is a global leader in Digital Risk Protection that works in partnership with some of the world's largest organizations to safeguard what matters most and defeat digital risk. Our solutions are a unique combination of proprietary data, technology, and human expertise to anticipate, identify, and remediate targeted threats to your executives, your brand, and your assets at scale—powered by the most extensive breach and social data collection from the surface, deep and dark web on the planet, with over 100B attributes and 45 billion curated identity records spanning 125 countries and 53 languages.

To learn more about how you can proactively anticipate, identify, and remediate targeted threats to your executives, your assets and your brand visit us at **constellaintelligence.com**

Why Constella

OUR TEAM

We're a diverse multinational team committed to becoming the most trusted global partner for defeating digital risk. Constella integrates interdisciplinary intelligence community analysts, infosec pioneers, military veterans, and tech entrepreneurs with advanced analysis of surface, deep, and dark web to protect what matters most.

OUR INSIGHTS

Our diverse team of expert multidisciplinary cyber intelligence analysts delivers real-time, actionable insights to identify threats and reduce risks emerging from the surface, deep, and dark web.

OUR DIFFERENCE

Our unique technology empowers advanced analysis across the entire risk surface for superior anticipation, protecting organizations, their individuals, and their critical assets. Because, the best way to overcome future threats is by facing them today.