



Cyber Security Journal

Ideas and insights on digital security to help
you safeguard what's most important to you

A low-angle, upward-looking photograph of several modern skyscrapers with glass facades. The buildings are framed by a bright blue sky with scattered white clouds. The perspective creates a sense of height and architectural complexity, with the grid-like patterns of the windows and structural beams converging towards the top of the frame.

Mobile in the Spotlight

How to stay safe
away from the
office and on
the road

BEC 2.0

Insights for
protecting
against a
sophisticated
and effective
cyber crime

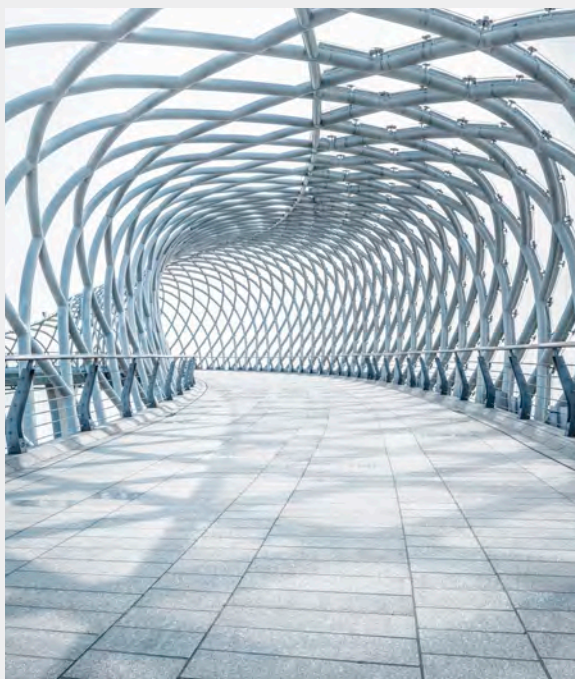
Contents

Cyber Security Journal • Vol. / One

Letter

3 From Craig Froelich, Chief Information Security Officer

Features



4

Mobile in the Spotlight

The coronavirus outbreak has restricted travel, made working remotely a necessity for many employees and increased risk as more mobile devices connect to company networks than ever before. But the right combination of tools and practices can help all organizations stay safe in uncertain times.



9

Business Email Compromise 2.0

Criminals are refining their methods and exploiting disruptions caused by the coronavirus to make this established cyber crime even more effective. Smart defense depends on being aware of how bad actors mimic our standard practices and capitalize on our willingness to trust.

Neither Bank of America nor its affiliates provide information security or information technology (IT) consulting services. This material is provided "as is," with no guarantee of completeness, accuracy, timeliness or of the results obtained from the use of this material, and without warranty of any kind, express or implied, including, but not limited to warranties of performance, quality and fitness for a particular purpose. This material should be regarded as general information on information security and IT considerations and is not intended to provide specific information security or IT advice nor is it any substitute for your own independent investigations. If you have questions regarding your particular IT system or information security concerns, please contact your IT or information security advisor. © 2020 Bank of America Corporation. All rights reserved. 3055721 EXP 2021-04-28.

Our commitment to you is absolute



Craig Froelich


Information security is a top priority for Bank of America because the trust of our clients and customers is fundamental to our business. Our approach to information security and data protection is an integral part of every system, process, and business interaction. Every product we build and program we launch has security at its foundation.

We want you — our clients — to trust in our ability to prepare, prevent, detect, mitigate, respond to and recover from information security threats and risks. We will continue to make the required investments in our technology and people to provide an evolving, multi-layered defense.

We also want to help you understand how to protect yourself and your company from cyber threats with the most current information available. To that end, we hope this publication will expand your knowledge of the latest threats and defenses. Each issue will explore current cyber security topics and actions you can take to mitigate risk. We are committed to sharing our knowledge and expertise to help protect you, your business and the broader community.

A handwritten signature in black ink, appearing to read 'Craig', with a large, stylized loop at the end.

Chief Information Security Officer, Bank of America



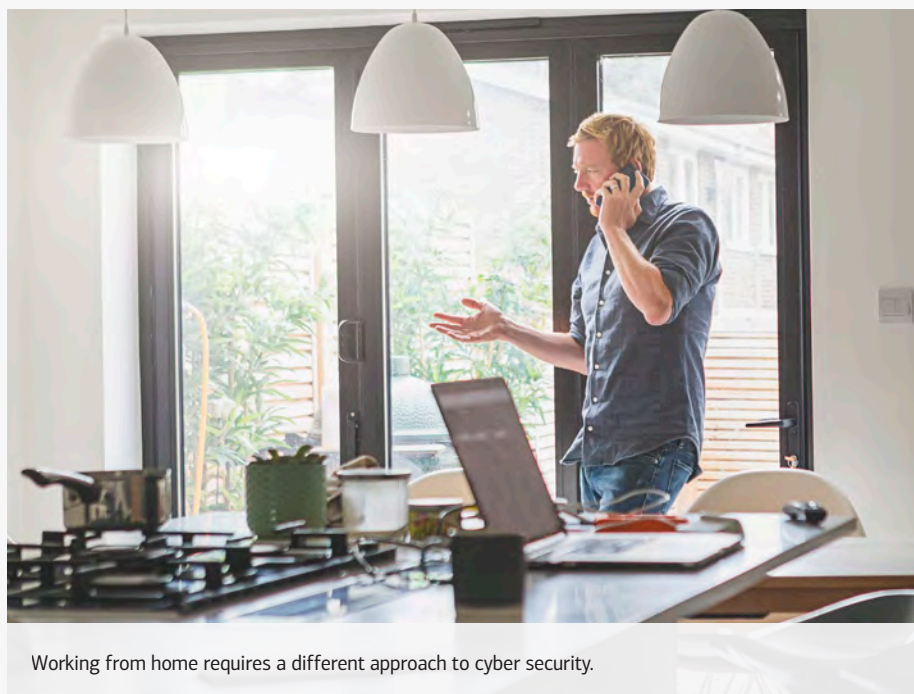
FEATURE ONE

Mobile in the Spotlight

Mobile devices and remote connectivity are business essentials, especially while the coronavirus disrupts operations worldwide. Working from home creates many new cyber security challenges, but enterprises can still keep their data and personal information safe.



Mobile in the Spotlight



Working from home requires a different approach to cyber security.

Cyber Security Journal
Vol. / One

they would not typically use so intensively and whose security features may be unfamiliar.

In many ways, the cyber security concerns presented by these conditions are simply the most recent evolution in the security landscape, in which some types of cyber events surge while others become less common. The mobile and personal devices and connections we depend on remain vulnerable to phishing, smishing (which targets short messages like texts), man-in-the-middle

attacks, data loss and other incidents that can compromise company networks and assets — whether we're working from home or, eventually, traveling for business again. Cyber criminals recognize that concerned, distracted and disrupted home-bound workers are vulnerable, and are launching malware campaigns targeting people who are working with insufficiently secured devices.

Yet despite criminals' opportunism, companies and their remote employees shouldn't have to sacrifice connectivity to maintain cyber security. With proper awareness, preparedness and a proactive, sensible attitude, remote and traveling workers can maintain productivity without increasing risk.



Imagine a finance executive in her makeshift home office, from which she's conducted every meeting and work task since her company sent all employees home in response to the coronavirus. She uses her personal mobile phone, her company's virtual private network (VPN), her home's internet service provider (ISP) for internet access and bridge lines to conduct group meetings. It's all technology she's used for years, but under the current circumstances she's setting up more meetings than usual and hasn't taken steps to secure them all, allowing unauthorized employees and threat actors to access meetings and overhear sensitive information.

Or consider an account manager frustrated by poor internet connectivity in his apartment, who emails documents with sensitive client information to a colleague using his mobile phone's hotspot. He uses a simple password for the hotspot, which an opportunistic cyber criminal is able to exploit to intercept the email and gain access to its contents, setting off a security breach that compromises both the account manager's company and several of its vendors.

These very different scenarios illustrate just two of the cyber security hazards that have become more common since the coronavirus response has required millions of workers to abandon their offices and set up in their homes, often with devices and tools

“With proper awareness, preparedness, and a proactive, sensible approach to cyber security, employees at home and on the go can maintain safe connectivity.”

Mobile device management is and will remain essential

Many organizations already have security tools and protocols in place for mobile devices and business travel that can apply to the current, massive growth of the remote workforce. However, businesses need to

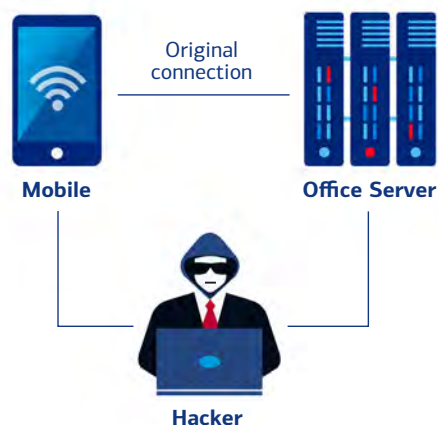


Mobile in the Spotlight

Cyber Security Journal
Vol. / One

The Evolving Mobile Device Threat Landscape

Whether you're working remotely because of a public health crisis or because you're traveling for business, you're utterly reliant on mobile devices. Here are some common threats to be aware of.



1 Phishing and smishing

Mobile email and text messaging scams can be effective on mobile device screens that may cut off key message details.

2 Vishing

Cyber criminals use tactics such as pretending to be a trusted source and robocalls with urgent messages to scam people out of data and money.

3 Malware

Spyware, banking malware, ransomware and adware can be designed to target personal and company-issued phones and weaknesses in mobile apps.

4 Compromised app cryptography

Criminals may access backdoors and weak app encryption to bypass a user's login credentials.

5 Network spoofing

Cyber criminals may set up fake Wi-Fi hubs to pry passwords and personal details from unsuspecting travelers.

6 Data leakage

Data can be lost or compromised by sending a message to the wrong recipient, or falling for spoofing, phishing or smishing attempts.



Mobile device management (MDM) combines centralized control with user options.

assess how much disruption current circumstances have created. Each organization will need to decide if their current security layers are sufficient and how familiar employees are with their use.

It's reasonable to expect that enforced remote work practices will only increase employees' reliance on mobile phones, whether they're working exclusively from home or in public areas. Because of this, mobile device management (MDM) remains critical to many cyber security strategies. MDM depends on a central server, which pushes updates and security features to built-in receptors on all company-issued devices. It can provide visibility into who's using mobile devices, as well as how and where they're using them. IT administrators and device owners also can deploy remote wipes, which can erase data or restore factory settings on lost or stolen devices. Organizations also can evaluate MDM solutions by how well they integrate with other business systems, how often their employees travel and by cost and support options.

There also are many mobile tools with software that loads directly on the device. Mobile threat detection (MTD) products can detect hazards such as phishing attempts or weaknesses in downloadable apps. Device encryption can make any stored data impossible to read, even if it is stolen. Data-loss prevention (DLP) software, which protects company data based on its value or confidentiality, can also improve overall visibility into data access and prevent unauthorized transfer.

Mobile virtual private networks (VPN) solutions, which cre-



Mobile in the Spotlight

Cyber Security Journal
Vol. / One



Virtual private networks (VPN) are critical for remote workers using sensitive data.

“In extraordinary circumstances, such as during the coronavirus pandemic, organizations should prepare accelerated and ongoing training to help employees protect against new threats.”

vide guidelines on the safe use of public Wi-Fi (when applicable), prohibit workers from transmitting sensitive information over anything besides company-issued devices and mandate the use of VPNs and well-protected home routers. If employees must travel, they should keep mobile device software, such as anti-virus tools, up to date, disable file sharing and avoid use of public charging stations that might expose their devices to malware infection (so-called “juice jacking”).

When employees work from home, it’s imperative for them to continue following company policies and not revert to shortcuts or relax security awareness. All business should be conducted on company-issued devices whenever possible, and employees should not allow other members of their households to access these devices for any reason. Password managers, multi-factor authentication, auto-updates and regular patches are all critical to secure remote connectivity, although employees who handle sensitive data or finances may need to invest in extra protec-

ate a secure, encrypted connection over public networks between a device and a company server, also have proliferated in recent years. These may be particularly valuable to employees who must access financial documents and accounts remotely. However, remember that no VPN solution is perfect, and some are better than others at securing data and maintaining privacy.

When employees are free to travel, physical tools such as display privacy filters and hardware-based authentication add an extra security layer. Basic behavioral defenses — keeping your devices in sight and locked when they aren’t in use, and utilizing biometrics whenever possible — are also essential, and employees must be encouraged to practice them.

Update and enforce a security policy for remote connectivity

Policies founded on good cyber security hygiene create another strong line of defense. Generally, company policies should pro-

Is Your Home Office Cyber-Secure?

If you’re required to work remotely, you can protect company data and assets with these precautions.



- 1 Follow all company data privacy policies.** If you must print hard copies of company files, keep your family from viewing them and securely dispose of these files after use.
- 2 Protect your router and physical work-space.** Make sure your screens are not visible from outside your home and change your default router passwords.
- 3 Do not allow anyone else to use your work-issued devices for any reason,** and power down all such devices when they are not in use.
- 4 Utilize all layers of your company’s security apparatus,** including VPNs, MDM, DLP and other security tools, and update software and security patches regularly.



Mobile in the Spotlight

Cyber Security Journal
Vol. / One



Organizations should maintain consistent messaging that highlights remote cyber security.

tion, such as a company-issued router that does not broadcast its service set identifier (SSID) and provides more robust security features. Companies with internal IT departments should encourage employees to set up consultations with knowledgeable staff if they have questions about their remote security apparatus.

Persist in training and education

When it comes to cyber security, there's always something new to learn, especially when work protocols are disrupted and decentralized. With most if not all employees stationed out of the office, compa-

nies must supply reminders on the basics of mobile security hygiene, especially to those employees who are unaccustomed to working outside the office and who are newly exposed to mobile device security threats.

Under normal conditions, employers should offer a cyber security refresher program at least once a year. In extraordinary circumstances, such as during the coronavirus pandemic, organizations should prepare accelerated and ongoing training to help employees

protect against new threats (such as disaster-response phishing emails or spoofed informational websites).

An overarching benefit of regular cyber security training is that it can help foster a culture of security across the organization. Once employees understand the inherent risks associated with mobility, it becomes easier to institutionalize smart cyber security messaging.

No matter what training method a company deploys, its messaging should be direct, focused and relatively simple. Armed with a few essential directives — such as staying off public Wi-Fi, making sure bridge connections are locked and not using personal devices except when necessary — employees can improve their chances of staying secure and protecting critical assets and information.

Align mobile solutions to business priorities

There is no one right way for companies to implement mobile and remote cyber security, especially during highly disruptive events. Conditions in newly created home offices, sensitivity of data, IT resources and level of employee training all may factor into a remote security strategy that's right for your particular company and its specific needs.

Yet any strategy will still rely on fundamentals. Driving home basics of cyber hygiene — thinking before clicking, using strong passwords, regularly backing up to company servers and investing in the right security tools — will pay dividends even after business is, once again, “as usual.” ■

Mobile in the Spotlight

Key takeaways:

- Review your MDM: Every company's needs are unique.
- Create a home office security checklist for all employees.
- Update training guidelines regularly but keep messaging simple.



FEATURE TWO

Business Email Compromise 2.0

Advanced tactics for business email compromise show that cyber criminals are becoming more sophisticated — but it's not all about the technology.



Business Email Compromise

Cyber Security Journal
Vol. / One



More than any other cyber crime, business email compromise (BEC) relies upon exploiting people's impulsive actions or willingness to trust. This is especially true during disruptive circumstances, such as the coronavirus pandemic. As offices close and millions of employees establish themselves in remote working environments, cyber criminals are crafting new BEC scams that may be sent to many employees besides financial decision-makers and other common targets.

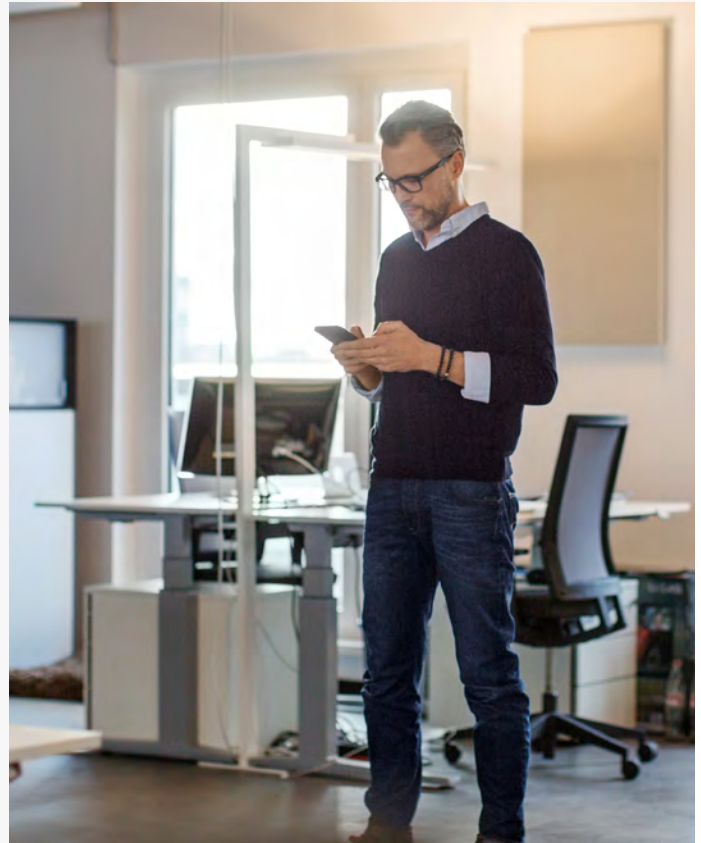
What's more, it's not just large corporations that are at risk. Cyber criminals routinely target leading internet companies, venture capital firms, small- and mid-size businesses in many industries, public school districts and even churches.

Opportunistic criminals are tailoring BEC campaigns that reference the latest coronavirus news, ask for donations and address institutional changes to payment schedules created by disrupted workflows. But a wide array of established scams that predate the pandemic continue to be effective. The FBI announced that total financial losses attributed to BEC incidents topped \$1.7 billion in 2019, a 37% spike over the year before. Since the overall number of BEC attempts is decreasing, evidence suggests that cyber criminals' methods are becoming increasingly nuanced and effective.

BEC scams often don't need to be particularly sophisticated from a technical perspective in order to work — they simply rely on tricking someone into taking an action. Humans are busy, easily distracted and rely on trust to get business done.

“BEC scams need not be technically sophisticated. They work because humans are busy, easily distracted and rely on trust to get business done.”

The disruption to normal business caused by the coronavirus just provides another layer of concern and distraction. In many successful scams, understanding and exploiting the psychology that motivates a person — or social engineering — matters almost as much as the technology used. Often, if BEC is successful, the target will have no idea what happened and will think they were just doing their job.



New BEC scams are using coronavirus news to lure targets.

Cyber criminals are utilizing a wider range of information sources to create and build their intricate email lures. Today's criminals scrutinize Securities and Exchange Commission financial statements and requests for proposals for email accounts, study roles and responsibilities listed in LinkedIn profiles and use open-source news to gather intelligence. They may also scour social media sites to glean personal details about targeted individuals.

“This deep research allows criminals to understand how a target interacts with others on the team, enabling them to add personalized details that lend credibility



Business Email Compromise

Cyber Security Journal
Vol. / One



Cyber criminals study corporate culture to craft BEC messaging.

“Deep research allows criminals to understand how a target interacts with others on the team, enabling them to add personalized details that lend credibility to the email. They tailor messages to build trust, which is essential to a successful BEC scam.”

if it is recurring. In these cases, the same individual might be victimized repeatedly. And with disruptions to business as usual caused by the pandemic — with many employees working from home, following new protocols and dealing with anxiety — the risk of anomalies going longer without being flagged may increase.

The expanding threat model

Historically, BEC has targeted financial gatekeepers like CEOs and CFOs. But cyber criminals' targets now encompass multiple functions across the business as well as third-party partners and international supply chains, which deepens the pool of potentially valuable targets.

The FBI recently reported an increase in payroll diversions that resulted from cyber criminals targeting payroll and human resources employees. In this type of scheme, criminals impersonate employees who are requesting changes in pay deposit accounts. The changed account information typically directs payments to bogus third-party accounts, which in addition to the theft results in missed paydays for the impersonated employees.

Also on the rise are incidents in which cyber criminals impersonate a trusted vendor or supply-chain partner to convince the company to make payments for contracted services. Criminals are looking

Continued on page 13

to the email,” says one cyber crime prevention officer. “They tailor messages as much as they can to the individual to exploit trust, which is essential to a successful BEC scam.”

It's clear BEC scammers are also polishing their writing skills to make fraudulent emails more difficult to detect. They are improving their grammar and spelling and reducing the use of idiomatic language to craft more authentic-sounding messages.

In addition, cyber criminals are now using compromised email accounts, rather than spoofed domains or doctored email headers, to craft messages that mimic the linguistic tone of a target or impersonate an employee or vendor. Access to those compromised email accounts also can unlock a trove of information contained in calendars, contacts and detailed company conversations.

BEC scammers are also joining forces with organized crime groups to share information on techniques to gain access to corporate email. The crime groups help BEC scammers locate and purchase stolen user credentials to take over email accounts.

These trends are compounded by the fact that it's taking longer for companies to detect BEC incidents, which gives criminals more time to harvest company information and gain access to funds. “Even large, very sophisticated organizations with multi-layer defenses against phishing and malware often fail to quickly detect BEC attempts because they don't pay attention to social engineering,” the cyber crime prevention officer says. In a department that disburses funds on a daily basis, one payment among many won't necessarily be flagged, even



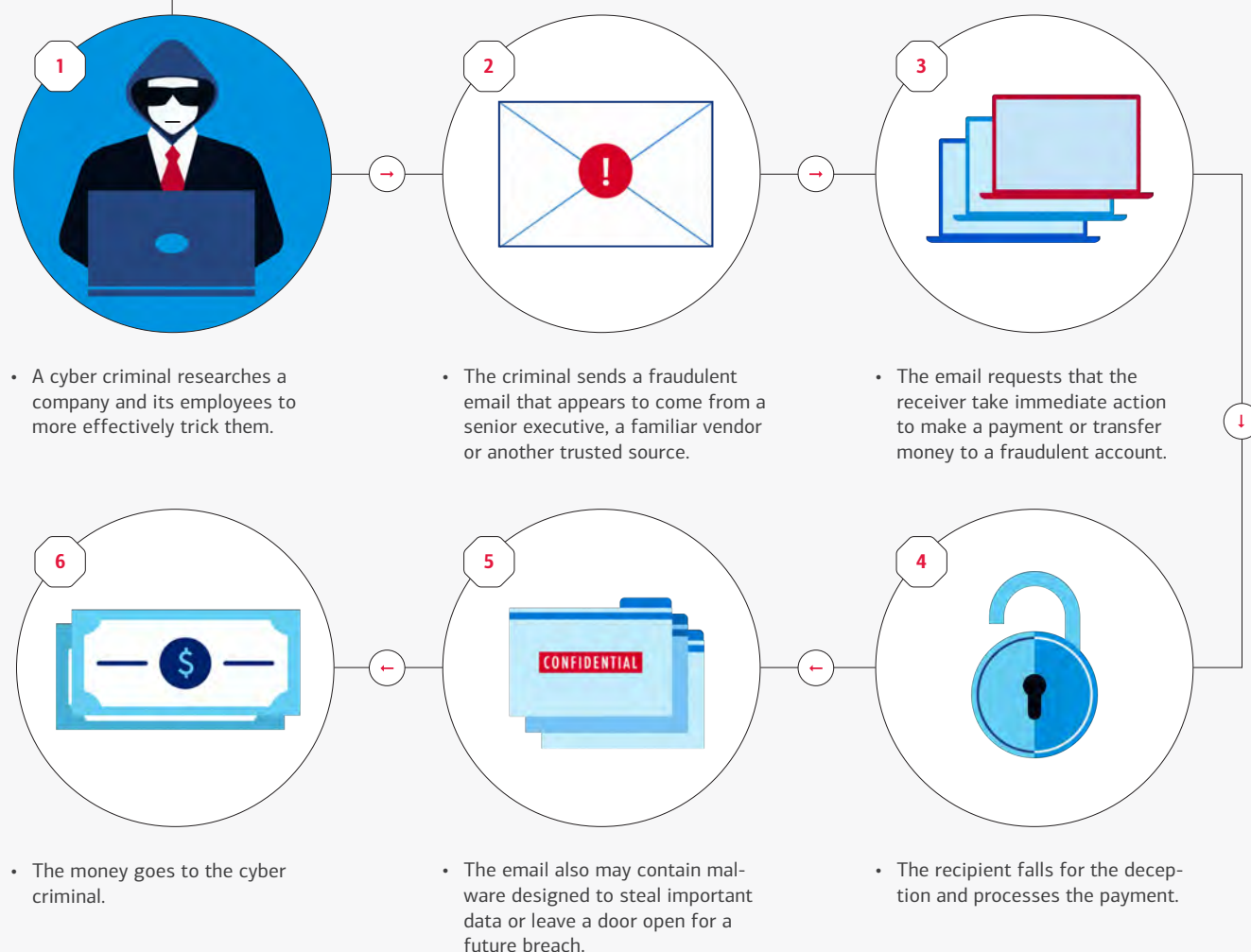
Business Email Compromise

Cyber Security Journal
Vol. / One

An increasingly effective cyber crime

BEC scammers change tactics based on current events, but the underlying strategy is consistent. No matter what type of messaging they use, cyber criminals launch BEC scams with tried and true formulas based on their knowledge of work protocols and human psychology. Ultimately, human error is just as critical to their success as any technical expertise.

How it works:



To protect yourself

- **Confirm** any unusual money requests in person or on the phone. Immediately report suspicious emails in accordance with your company's guidelines.
- **Verify all details** in emails from unknown individuals and do not send sensitive information to anyone whose identity you can't confirm.
- **Don't reply** to emails from people you don't know or click on links or attachments in those emails.

If you think you've been targeted

- **Call your bank** and freeze financial accounts that may be affected, inform credit bureaus and change passwords that may have been breached.
- **Document everything** about the incident. The more information you have to share with law enforcement, the better armed you will be to assist an investigation and the better prepared you will be against future cyber incidents.
- **File reports** with the relevant local authorities.



Business Email Compromise

Cyber Security Journal
Vol. / One



Social engineering tactics are increasingly subtle and effective.

Social Engineering at Work

BEC scams fall into a few general categories, and all rely on keen observation of business behavior and human nature to succeed:



1. Vendor email compromise (VEC). A cyber criminal takes control of a legitimate email account in a company, and uses that account to target organizations across the company's supply chain by sending payment or account change requests.

2. Executive payment requests. Using a spoofed or compromised email, a criminal impersonating a supervisor requests an employee to make a fraudulent payment. Instructing

employees to purchase gift cards has become a prolific scam, particularly during holiday seasons when it's not out of place.

3. Payroll diversion schemes. A criminal pretends to be an employee and sends a request for a change in direct deposit account information, rerouting the real employee's paycheck to an account of their choice.

4. Legal, financial or data requests. After observing the typical patterns of a target's business transactions, or studying the terms of a public contract, criminals can send a fraudulent request for money at the exact moment when the business expects it.

Continued from page 11

at employee relationships up and down the supply chain to exploit the relationships between a business and its vendors.

Cyber criminals are also becoming more specialized by targeting specific industries. They increasingly are setting their sights on real estate and mortgage companies that handle escrow and mortgage payments. A common strategy is to take control of email accounts to learn the cadence of payments and then hijack the fund transfers using a man-in-the-middle technique, in which a criminal intercepts communications between two parties to disrupt traffic between them, steal data or load malware.

How you can battle BEC

Fending off BEC scams requires that businesses implement updated operational processes and provide ongoing training and awareness campaigns for employees.

It's critical to review the protocols and controls that govern how account information is updated and payments are approved for both domestic and international transactions. Requests to make payments or to change account information should be approved through a different channel than that of the original inquiry. Businesses should create and maintain a list of contacts and account information and provide a step-by-step response to BEC attempts to address awareness and defense.

To stem the flow of potentially sensitive personal and business information, companies should also ask employees with payment-making authority to limit what they post on LinkedIn and other social media sites.

Keeping employees current and (re)trained

It's important to note that even the most robust processes will

“Even the most robust cyber security processes will be ineffective against BEC scams without updated, continuous cyber security training and awareness programs for all employees.”

be ineffective without continuous cyber security training and awareness programs. Organizations should train employees across functions to create general awareness of BEC threats and techniques. Employees who are among the likeliest to be targeted — CEOs and CFOs (and their personal assistants), finance department personnel, payroll staff and



Business Email Compromise



A 'trust but verify' approach helps employees detect fraudulent emails.

HR officers — should receive more in-depth training.

While these defenses are primarily process-driven, certain technologies can supplement a robust anti-BEC strategy. Cyber crime prevention officers recommend using email filtering technologies that analyze incoming messages for suspicious header and domain information. For example, if the filtering tool alerts you that an email from the company CFO was sent from an external account, that's an immediate tip-off that should prompt you to verify the request with the CFO directly.

Treat BEC as a human — and technological — problem

No matter what a company's technological preferences and budgets may be, impersonation, coercion and the human tendency to trust are essential for cyber criminals to successfully carry out fraud campaigns, including BEC. As a result, these factors are equally vital to any effective BEC and cyber crime defense strategy. Many social engineering tactics can be neutralized with a "trust but verify" approach to business communication that applies to both internal and external channels.

As email-based scams continue to improve and evolve to take advantage of disrupted work practices, businesses will need to remain responsive and proactive. It will be critical that they take the steps necessary for implementing processes to help prevent and respond to incidents, as well as develop comprehensive employee awareness programs that illustrate the latest techniques used by cyber criminals. Doing so can help protect susceptible employees and company resources. ■

BEC 2.0

Key takeaways:

- BEC depends on human error and willingness to trust.
- Cyber criminals study their targets before launching an attack.
- BEC attempts often target mobile devices and on-the-go employees.

Cyber Security Journal
Vol. / One

BEC Facts:

Statistics show BEC attempts are becoming more targeted and successful



\$1.7 billion

Total losses in the U.S. attributed to BEC in 2019, a 37% increase over the year before.

No. 1

The rank of the U.S. among countries most targeted by BEC scammers.

Top 10

BEC email subject lines

Transaction request
Important
Urgent
Request
Payment
Outstanding payment
Info
Important update
Attention
Notification of payment received

Sources: FBI Internet Crime Complaint Center, 2019 Internet Crime Report, February 2020; Symantec, "BEC Scams Remain a Billion-Dollar Enterprise, Targeting 6K Businesses Monthly," July 23, 2019