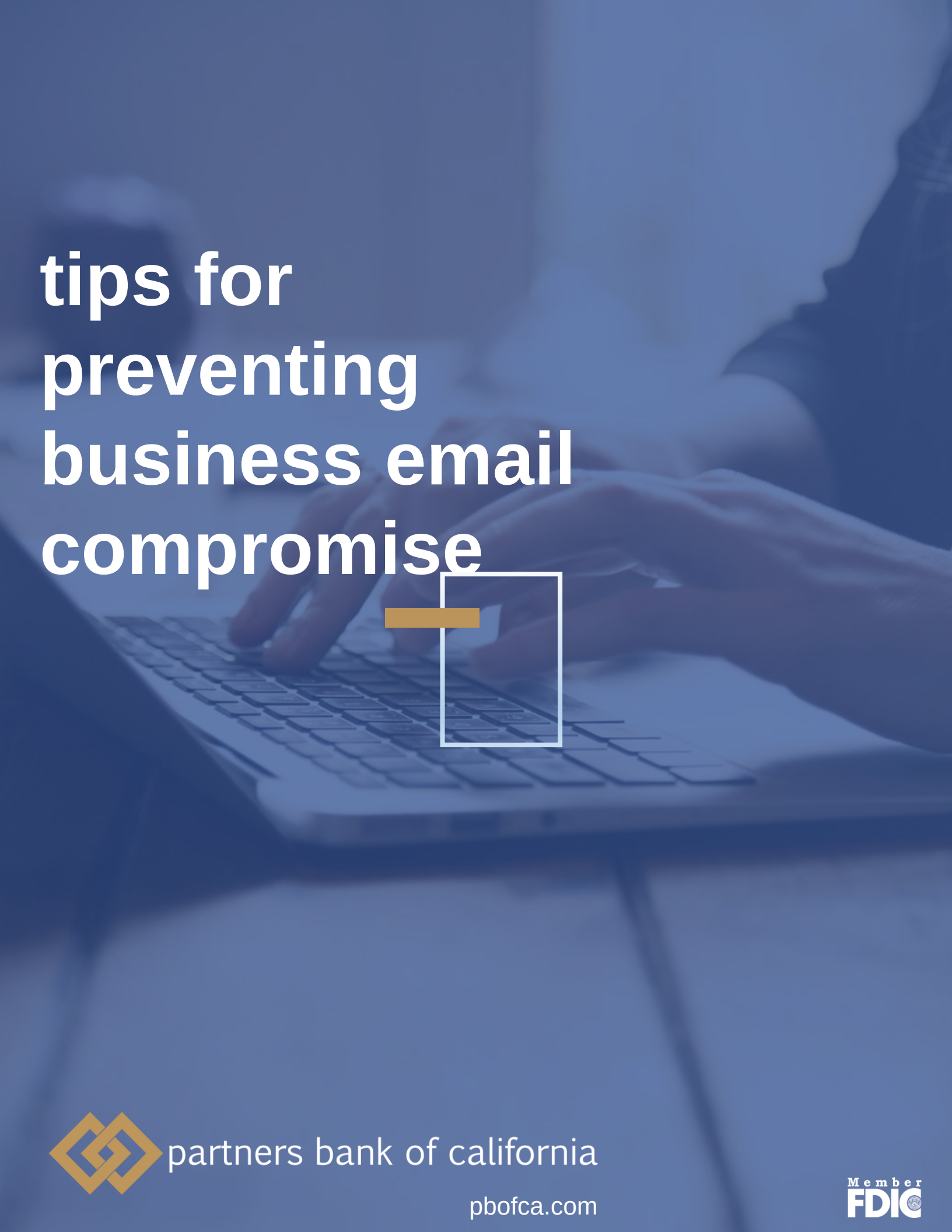


tips for preventing business email compromise

partners bank of california

pbofca.com

Member FDIC

tips for preventing business email compromise

what you need to know

introduction

Businesses can always take precautions and deploy security measures to prevent Business Email Compromise (BEC), and many do. However, the risk is always there. No matter how well people are trained, they will inevitably make mistakes; and those mistakes have the potential of causing irreparable harm to your organization because businesses are under attack 24/7.

The U.S. Treasury Department's Financial Crimes Enforcement Network (FinCEN) recently sent urgent and updated advisories to U.S. financial institutions regarding email compromise fraud schemes that target business processes. Those targeted 'processes' often involve financial transactions between your business and your bank.

BEC perpetrators identify vulnerable processes to compromise, and then insert themselves into communications by impersonating a critical player in the business relationship or transaction – a form of 'social engineering.' A scheme's probability of success and the potential payout from fraudulent payment instructions often depends on the criminals knowledge of the business's normal processes, as well as weaknesses in the business's authorization and authentication procedures.

Industries with public-facing information about their business transactions and processes can present attractive targets for BEC schemes. What's more, everything is mobile now. Employees who once used business-owned laptops and desktops to check their email now rely on their own mobile devices.

It might sound overwhelming when you compile all the BEC threat possibilities that are looming out there. In order to properly address the challenges that make businesses more vulnerable to financial losses stemming from BEC schemes, businesses must deploy measures to markedly strengthen email security. We've included tips to prevent email-borne attacks from reaching employees and to mitigate attacks that penetrate a business's processes.

Your online safety and financial health are very important to us. If you have any questions or need assistance regarding online security or any of our products and services, please give us a call at (949) 732-4000 or email us at onlinebanking@pbofca.com.

tips for preventing business email compromise

tip #1
talk about it and train your team

Help your employees to understand and recognize a possible business email compromise threat.

Your employees may be the last line of defense against a BEC attack on your business.

Email security training should be a regular and mandatory part of your business training program.

If you need training resources, SANS Institute (sans.org) also offers many free online security resources to businesses.

tips for preventing
business email compromise

tip #2

adopt stronger encryption and web-based email

Transport Layer Security (TLS), formerly known as Secure Sockets Layer, protects all sessions using email protocols, including IMAP, POP and SMTP.

Using a web-based email service instead of locally installed email client software ensures TLS will protect web traffic.

Email encryption is recommended for use whenever your business is transmitting sensitive or confidential information via email, especially when transmitting financial or electronic funds transfer information between your business and your bank.

There are many reputable commercial email encryption services available. Consult with an IT professional for a recommendation on which system best serves your business's needs.

tips for preventing
business email compromise

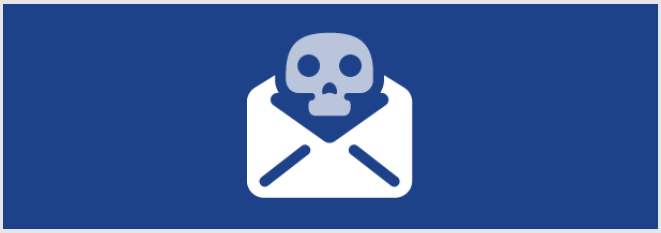
tip #3

move to modern anti-malware solutions

Newer anti-malware relies less on signatures of known malicious content and instead uses threat intelligence, reputation services and other near-real-time sources to pinpoint the location of threats such as domains, and IP and email addresses.

With highly target attacks now commonplace, it is vital to employ only anti-malware that uses the latest threat information.

Ideally, businesses should deploy modern anti-malware technologies as part of their infrastructure to monitor all email servers and services.



Each client device should also have anti-malware technologies installed in order to catch email-borne threats passing through outside email services.

tips for preventing
business email compromise

tip #4

initiate mandatory email client health checks

Businesses should monitor the health of all email client devices, whether company-owned or Bring Your Own Device (BYOD).

Automated health checks can flag problematic email accounts and identify emerging security problems, such as end-user systems that use weak security settings or lack operating system (OS), and email client software patches.

Automated health checks should also hasten correction action by your business's IT team.

Being proactive with the health of your email platform is critical to the prevention of BEC attacks.

tips for preventing
business email compromise

tip #5

block exfiltration with data loss prevention tools

Cyberthieves commonly use email as a preferred mechanism for exfiltration – the unauthorized transfer of sensitive information outside the business or organization.

Malicious insiders often use their email accounts to forward sensitive data files to other email addresses, and attackers use compromised accounts similarly. Data Loss Prevention (DLP) technologies can detect and stop these threats.

DLP is a critically important weapon in the email security arsenal.

Whenever possible, DLP tools should be used to monitor email servers and any client devices with access to sensitive data that might be an enticing target.

tips for preventing business email compromise

tip #6
install ‘whitelisting’ applications

There’s some bad stuff out there on the web, often lurking inside applications that could be launched unknowingly by a member of your team. Application whitelisting technologies allow only authorized software to execute.

Many desktop and laptop operating systems have built-in application whitelisting that when properly configured and maintained, can prevent malware and other unauthorized executables from running on devices.

Whitelisting provides a last barrier of defense – if malware gets through other security controls and installs on a device, it won’t be able to fulfill its mission.

A smartphone can be set to execute software only from an authorized app store, and all apps in that store can be screened for malware.