Here's what you NEED TO KNOW about business email compromise

Remember the old days when all of those Nigerian princes were emailing you to offer giant sums of money?

All you'd need to do, of course, was click that suspicious-looking link, share your bank account information and you'd be living large.

HOW do they HAPPEN?

The threat actors behind these campaigns create phishing emails with links to credential harvesting sites impersonating webmail login portals. The crafty attacker then uses the compromised credentials to access the victim's email through the corresponding legitimate webmail portal.

Depending on the victim's role in the org, the threat actor might:

Attempt to issue a fraudulent invoice or fraudulent wiring instructions; or

Send credential-harvesting phishing emails to all contacts in the victim's email address book to perpetuate the campaign.

What's a BUSINESS EMAIL COMPROMISE (BEC)?

The scam described above is the old school version of BEC, but BECs have grown up since then. They still start with an email and target people and organizations everywhere ... but they're a lot more sophisticated (and harder to spot). Most people think that BEC is synonymous with wire transfer fraud. But the reality is that BEC is much more -- it includes payroll, romance, real estate and lottery scams.

How FREQUENTLY do BECs happen?

A lot more often than you'd think.

OCT 2013 ⟷ **78,617** BEC incidents from ⟷ MAY 2018

+150 countries ⟷ **all 50** U.S. states

Source: https://www.ic3.gov/media/2018/180712.aspx

In a 3-MONTH period

58% of Expel customers experienced a BEC attempt in Office 365

37% of those customers experienced more than one BEC attempt

How can you DETECT A BEC?

Once an attacker compromises a user's account they'll start doing some things typical users won't do (including covering their tracks). To find them, look for suspicious user activity.

Here are a few things we typically watch for:

Inbox rules that automatically forward emails to hidden folders

Inbox rules that automatically delete messages

Inbox rules that redirect messages to an external email address

Inbox rules that contain BEC keywords (check out our full list of keywords)

New mailbox forwarding to an external address

Successful mailbox logins within minutes of denied logins

New mailbox delegates

Logins from proxy or VPN services

How can your team STOP A BEC?

Turn on multi-factor authentication (MFA)
38% of the attempted BECs could have been stopped by enabling MFA for Office 365

Watch your geolocation records
We detected 68% of these BEC incidents using geolocation records

Require a physical paper trail for wire transfers
For financial transactions over a certain size, require someone to put their signature on paper

Know the common BEC tactics attackers use
We detected 32% of the BEC attempts by alerting on tactics like inbox rules, folder redirection and delegation

expel

How can you make your org more resilient to BEC attempts?
Read all our pro tips for thwarting attacks at **www.expel.io/bec.**