KnowBe4
Human error. Conquered.

Get an Insider View Into the Methods and Exploits of the World's Most Famous Hacker

A Discussion with Kevin Mitnick

Kevin Mitnick
Chief Hacking Officer
KnowBe4, Inc.

Perry Carpenter
Chief Evangelist & Strategy Officer
KnowBe4, Inc.

About today's format...

This is not your typical webinar

Kevin Mitnick
Chief Hacking Officer
KnowBe4, Inc.

Perry Carpenter
Chief Evangelist & Strategy Officer
KnowBe4, Inc.

KnowBe4
Human error. Conquered.

What Would Kevin Do

- Don't allow employees to receive files with macros unless they are trained about the significant risks
- Utilize technical controls to limit Office macro use
  - Secure Email Gateway Products
  - Microsoft users can enable audit attack surface reduction rules

Article in Webinar Resources widget:

Audit Attack Surface Reduction Rules

What Would Kevin Do

- Phone pre-texting is a serious threat
  - Policy: If someone asks you for sensitive information or to do an action item, you should call the person back at a <u>verified number</u> before complying.
  - Specific verification policies may be needed for outside vendors so threat actors can't easily impersonate customers, suppliers, or vendors

What Would Kevin Do

- Remove PowerShell version 2
- Enable PowerShell logging
- Randomize local administrator passwords – Local Administrator Password Solution (LAPS) or privileged management tools
- Segment your network
- Disable wdigest authentication via the registry
- Segregate admin accounts
- Harden admin workstation; block all incoming connections using built-in Windows Firewall
- Utilize multi-factor authentication on <u>all</u> external resources
- Run Bloodhound to identify paths to Domain Admin
- TEST, HARDEN, AND TRAIN YOUR USERS – Stop and Think!

KnowBe4
Human error. Conquered.

Thank You

KnowBe4
Human error. Conquered.