Security Threat & End User Education

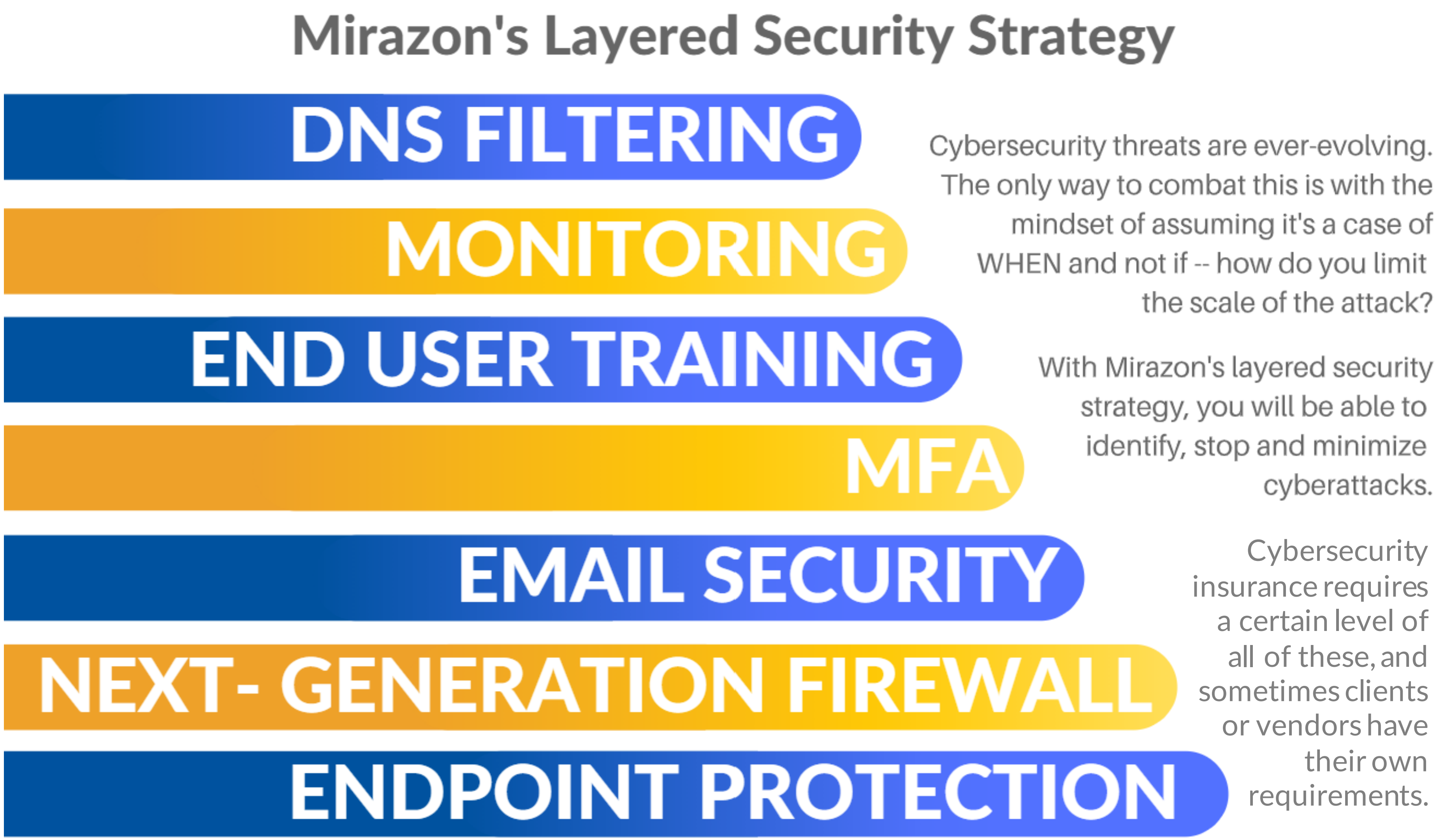
April 29, 2022

LouMUG

Agenda

- A layered security strategy
- Finding your weakest link in the security chain
- Security Awareness Training & Testing
- Manual vs automated testing
- Keeping up with threats
- Options for tools to combat
- Recommendations & resources

A layered security strategy



Mirazon's Layered Security Strategy

DNS FILTERING

MONITORING

END USER TRAINING

MFA

EMAIL SECURITY

NEXT- GENERATION FIREWALL

ENDPOINT PROTECTION

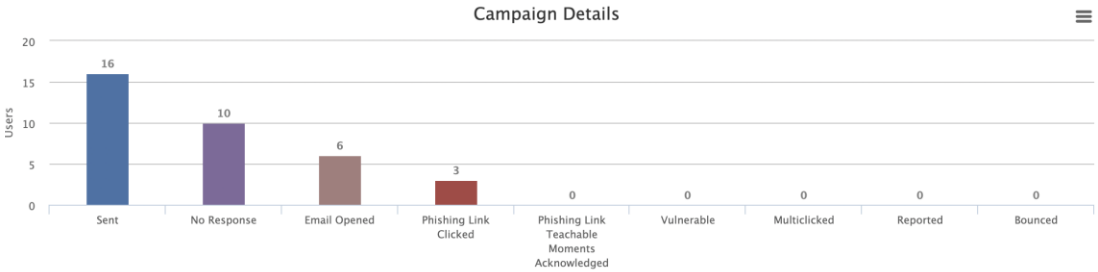
Cybersecurity threats are ever-evolving. The only way to combat this is with the mindset of assuming it's a case of WHEN and not if -- how do you limit the scale of the attack?

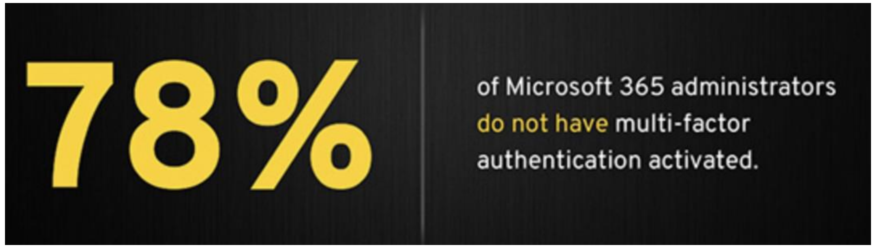
With Mirazon's layered security strategy, you will be able to identify, stop and minimize cyberattacks.

Cybersecurity insurance requires a certain level of all of these, and sometimes clients or vendors have their own requirements.

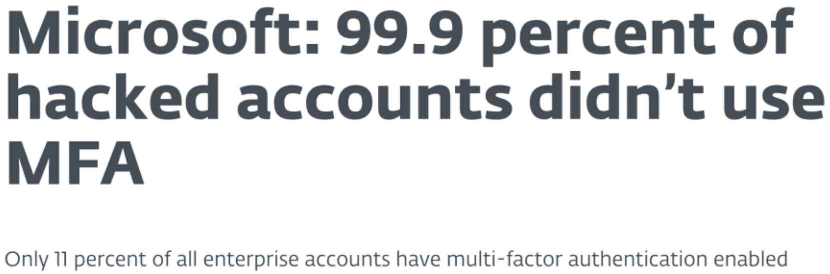
Finding your weakest link

- No amount of technology can 100% protect you from human factors.
- Not always the end-user…
- Sys Admins often get complacent despite being a prime target.
- Other factors like budget, management <gasp>, etc. can be a weak link.




78%

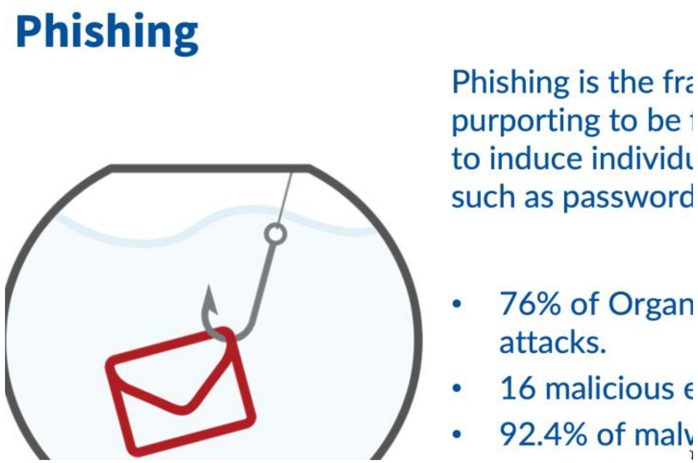
of Microsoft 365 administrators do not have multi-factor authentication activated.


Microsoft: 99.9 percent of hacked accounts didn't use MFA

Only 11 percent of all enterprise accounts have multi-factor authentication enabled

Security Awareness Training

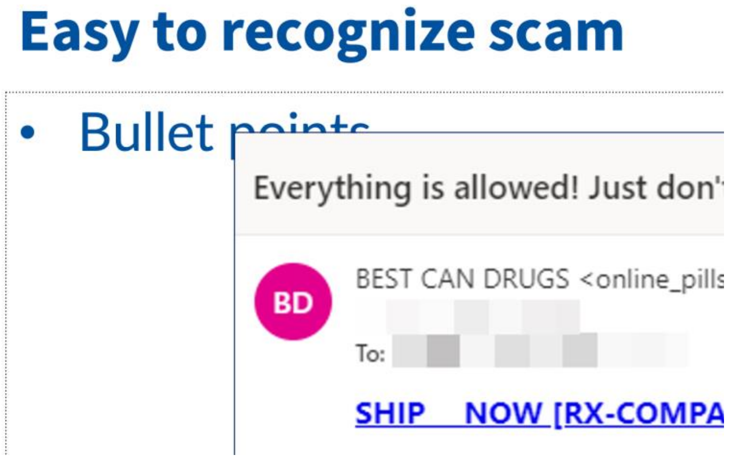
- Classroom Training
- On-prem or remote
- This is not a one-time thing, offer on a recurring basis
- Record your training for later viewing
- Know your audience
- Don’t be too technical
- Talk about why, and what’s in it for the end-users (protecting personal & home data)
- Make end-users part of the solution!



Phishing

Phishing is the fra
purporting to be
to induce individu
such as password

- 76% of Organ attacks.
- 16 malicious e
- 92.4% of malv



Easy to recognize scam

- Bullet points

Everything is allowed! Just don'

BD

BEST CAN DRUGS <online_pills

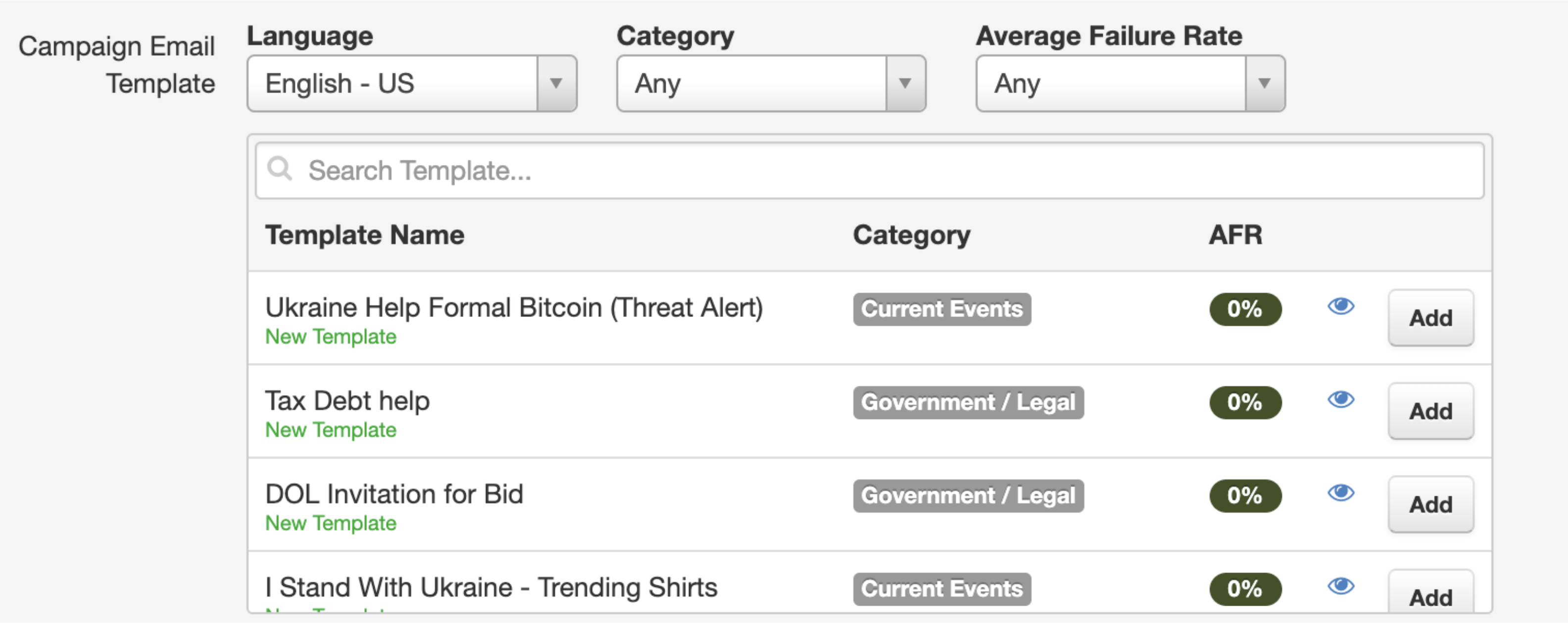
[redacted]

To: [redacted]

SHIP NOW [RX-COMPA

Security Awareness Testing

- What tools are available to automate this?
- Proofpoint SAT, KnowB4, M365 built in tools
- What are the campaigns?
  - Phishing
  - Embedded Links
  - Attachments
  - M365
  - Gift cards
  - Etc.



Campaign Email Template

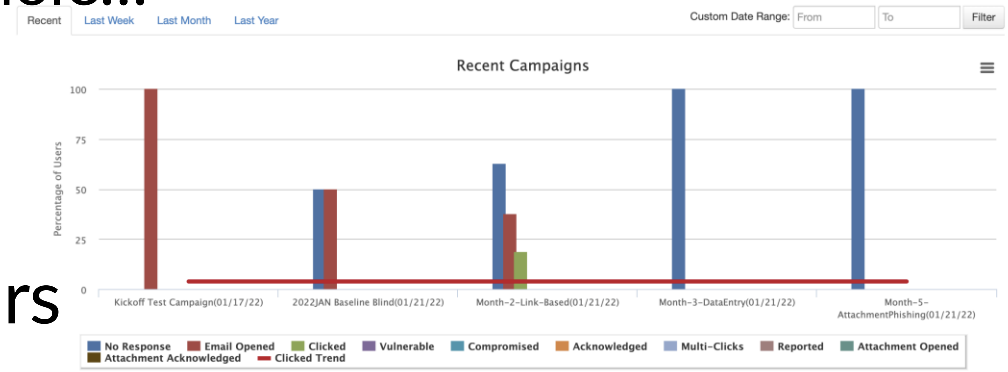
Language	Category	Average Failure Rate
English - US	Any	Any

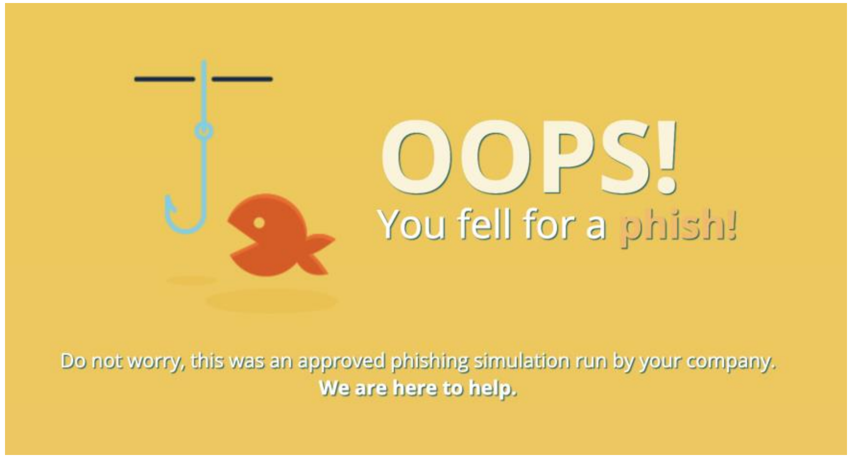
Search Template...

Template Name	Category	AFR		
Ukraine Help Formal Bitcoin (Threat Alert) New Template	Current Events	0%	👁	Add
Tax Debt help New Template	Government / Legal	0%	👁	Add
DOL Invitation for Bid New Template	Government / Legal	0%	👁	Add
I Stand With Ukraine - Trending Shirts	Current Events	0%	👁	Add

Manual vs automated testing

- User scoring/rating on admin console
  - How far did the user go down the rabbit hole…
    - Did they open the email?
    - Did they click the link?
    - Did they enter credentials?
- Real-time notification of failure for users
  - Screenshot here?
- Assign training/learning videos/quiz





OOPS!

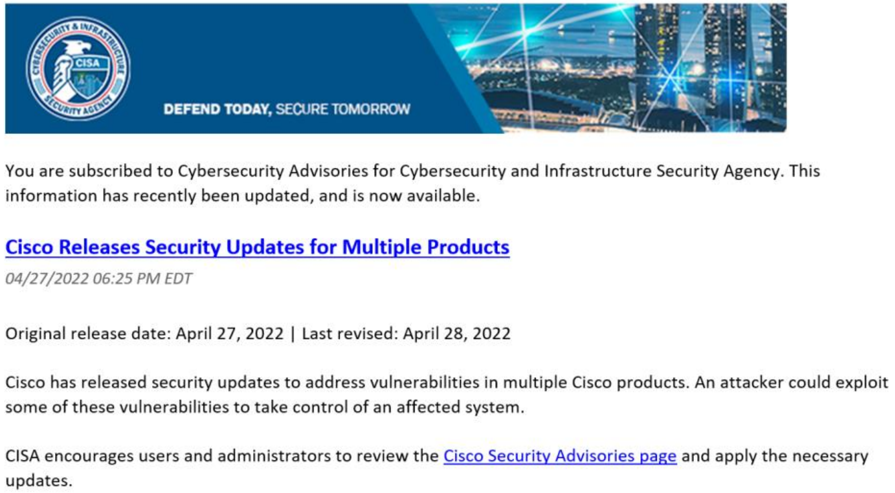
You fell for a phish!

Do not worry, this was an approved phishing simulation run by your company.

We are here to help.

Keeping up with threats

- Government Sites
  - CISA, DHS, NIST
  - US Cybercom
  - US State Department
- Vendor Notifications / Blogs
  - CrowdStrike
  - Fortinet
  - Veeam
  - Reddit
  - YouTube



You are subscribed to Cybersecurity Advisories for Cybersecurity and Infrastructure Security Agency. This information has recently been updated, and is now available.

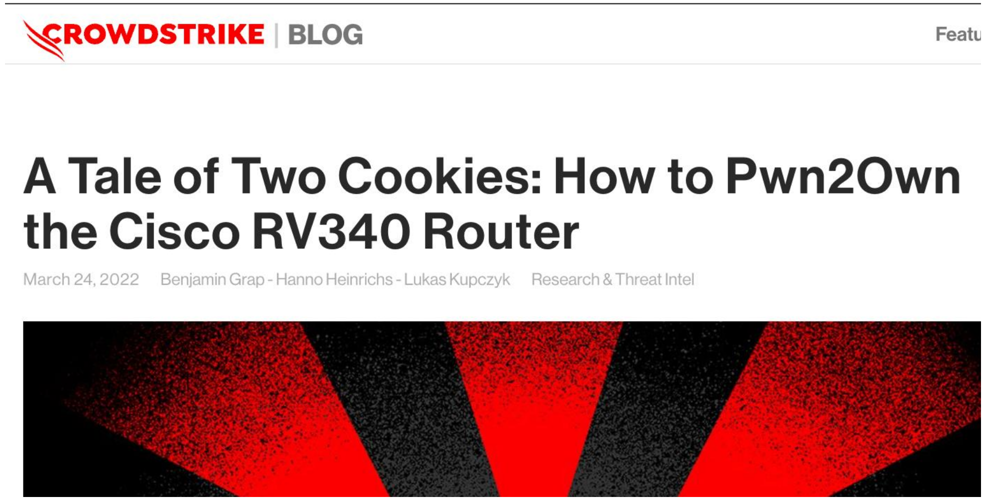
Cisco Releases Security Updates for Multiple Products

04/27/2022 06:25 PM EDT

Original release date: April 27, 2022 | Last revised: April 28, 2022

Cisco has released security updates to address vulnerabilities in multiple Cisco products. An attacker could exploit some of these vulnerabilities to take control of an affected system.

CISA encourages users and administrators to review the Cisco Security Advisories page and apply the necessary updates.



A Tale of Two Cookies: How to Pwn2Own the Cisco RV340 Router

March 24, 2022 Benjamin Grap - Hanno Heinrichs - Lukas Kupczyk Research & Threat Intel

Your Tools to Combat Threats

- We are all aware of AV, Firewalls, etc. but what else?
- OpenSource Distros (Kali, BlackArch)
- Free tools like Systinternals
- OSINT & social tools like SpiderFoot & Social-Analyzer
- Dark Web forums

Other Recommendations & Resources

- Open Discussion
- What have you learned along the way?
- What other security layers do you use?
- Share any cautionary tales.
- Any horror stories?

Thanks! Q&A

Presenter contact info here