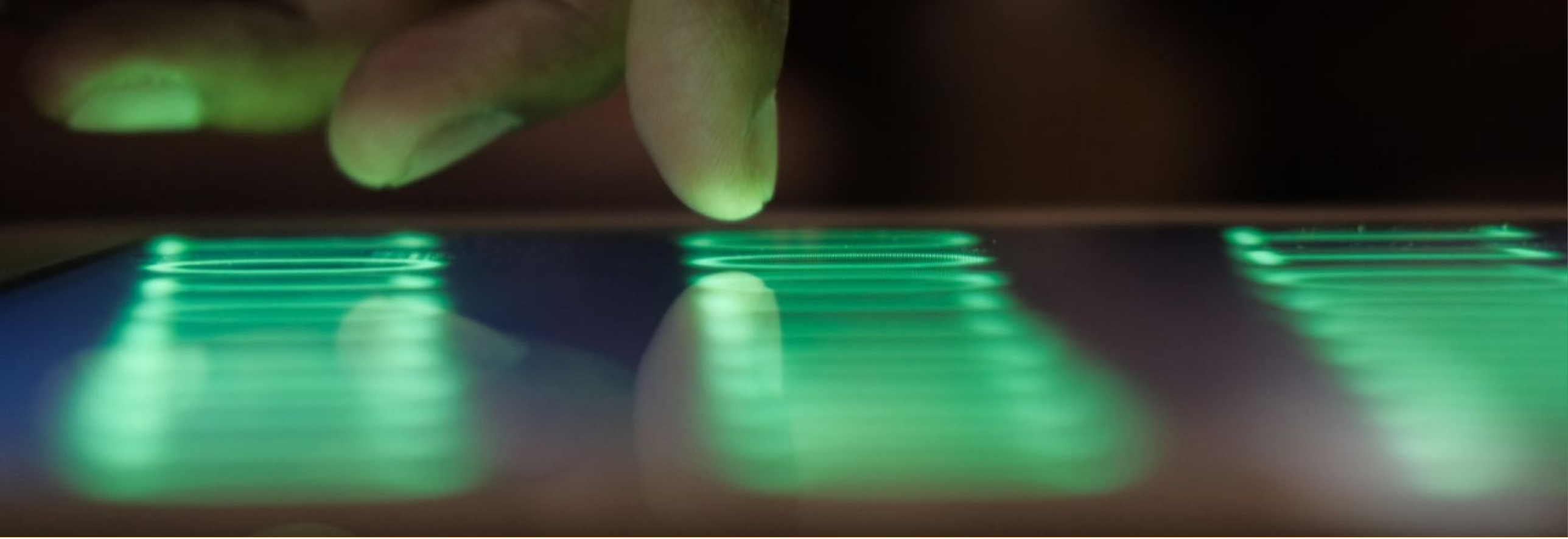


CommunityIT Innovators®

Protect your Nonprofit from Financial Fraud

Your Part-Time Controller®
The NONPROFIT accounting specialists™

February 16, 2022

CommunityIT Innovators®
where technology meets mission

Learning Objectives

1. Discuss the cybersecurity landscape and vulnerabilities for nonprofit organizations

2. Identify and define the types of cybersecurity incidents and discuss examples

3. Share tips and best practices for financial processes and IT tools to help prevent and detect fraudulent activity

YOUR PART-TIME CONTROLLER®
The NONPROFIT accounting specialists™

CommunityIT Innovators® where technology meets mission

About Community IT

100% Employee Owned

Advancing mission through the effective use of technology.

Channel Futures MSP 501 2019 WINNER

Today's Guest Presenter

Carole Melvin, CPA
Senior Manager Washington DC Office,
Your Part-Time Controller, LLC

Who We Are

YOUR PART-TIME CONTROLLER®
The NONPROFIT accounting specialists™

Almost 30 years serving non-profit organizations because we believe in their good work and missions.

Nine regional markets including a nationwide remote market through YPTC Anywhere℠.

A 'Best Place to Work' for over a decade. A 2021 *Accounting Today* Best Firm.

Working on-site and virtually.

Over 1000 clients building a better world.

300+ staff and growing.

Presenter

Matthew Eshleman
CTO

Poll #1

CommunityIT Innovators® where technology meets mission

Your Part-Time Controller® The NONPROFIT accounting specialists™

What is your role at your organization?

- IT department
- Finance
- Operations
- Admin

Agenda

- Cybersecurity Landscape
- Wire fraud
- Examples
- How to protect your org

1

Cybersecurity Landscape

Vulnerabilities for Nonprofit Organizations

CommunityIT Innovators®
where technology meets mission

YOUR PART-TIME CONTROLLER®
The NONPROFIT accounting specialists™

CYBERSECURITY LANDSCAPE

CommunityIT Innovators® where technology meets mission

Persistent and ongoing brute force attacks on identities

Sophisticated spearphishing

Attacks targeting organizations because of the work they do

Schemes targeting vendors

CYBERSECURITY LANDSCAPE

Entities are not always aware of new security tools available to combat emerging cyber threats.

Nonprofit organizations generally have fewer cybersecurity fraud controls in place

68% of Nonprofits don't have an Incident Response Plan

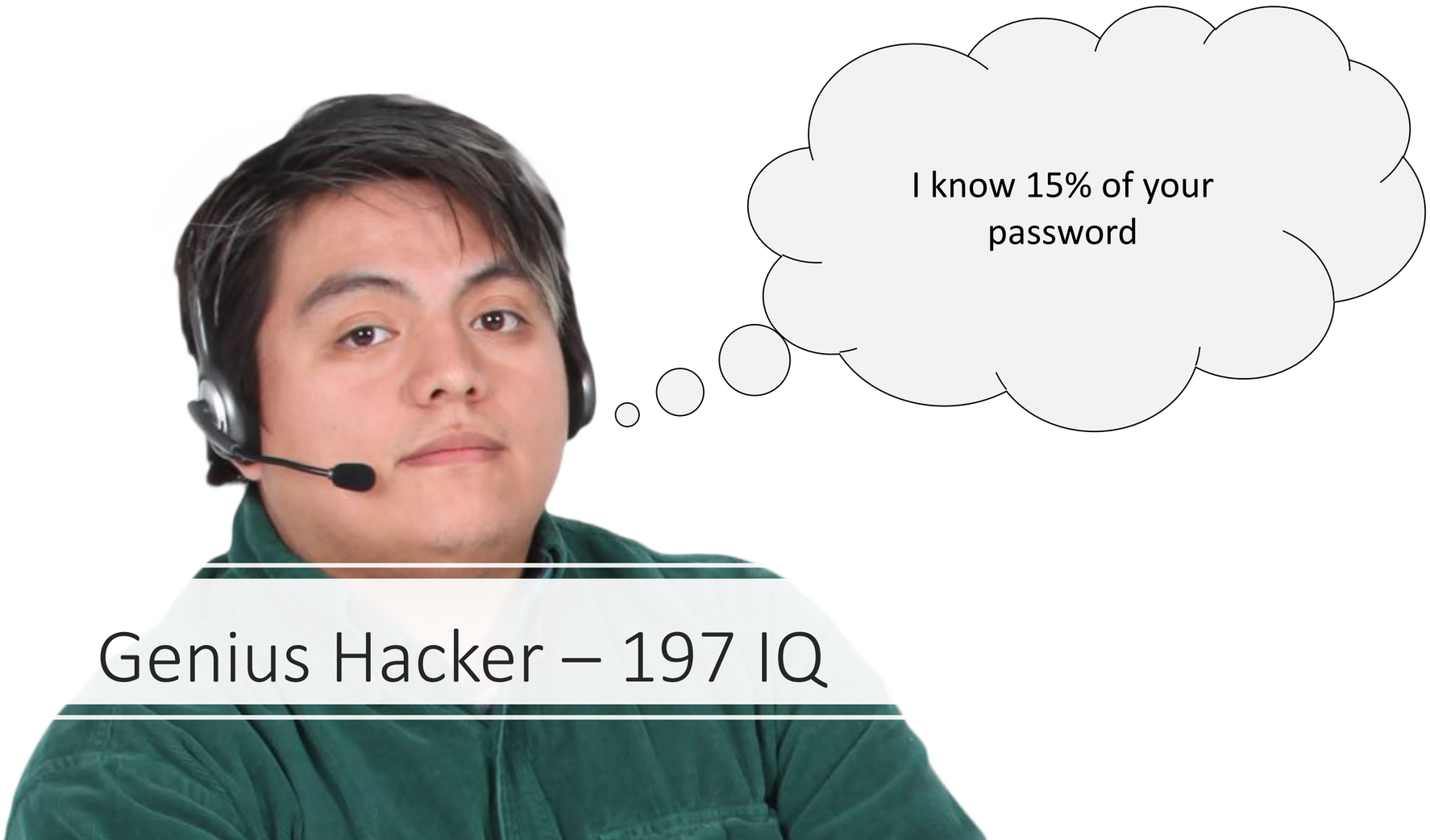
Breach response for a small to medium business is $149,000

CYBERSECURITY LANDSCAPE

165% change

https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

CYBERSECURITY LANDSCAPE

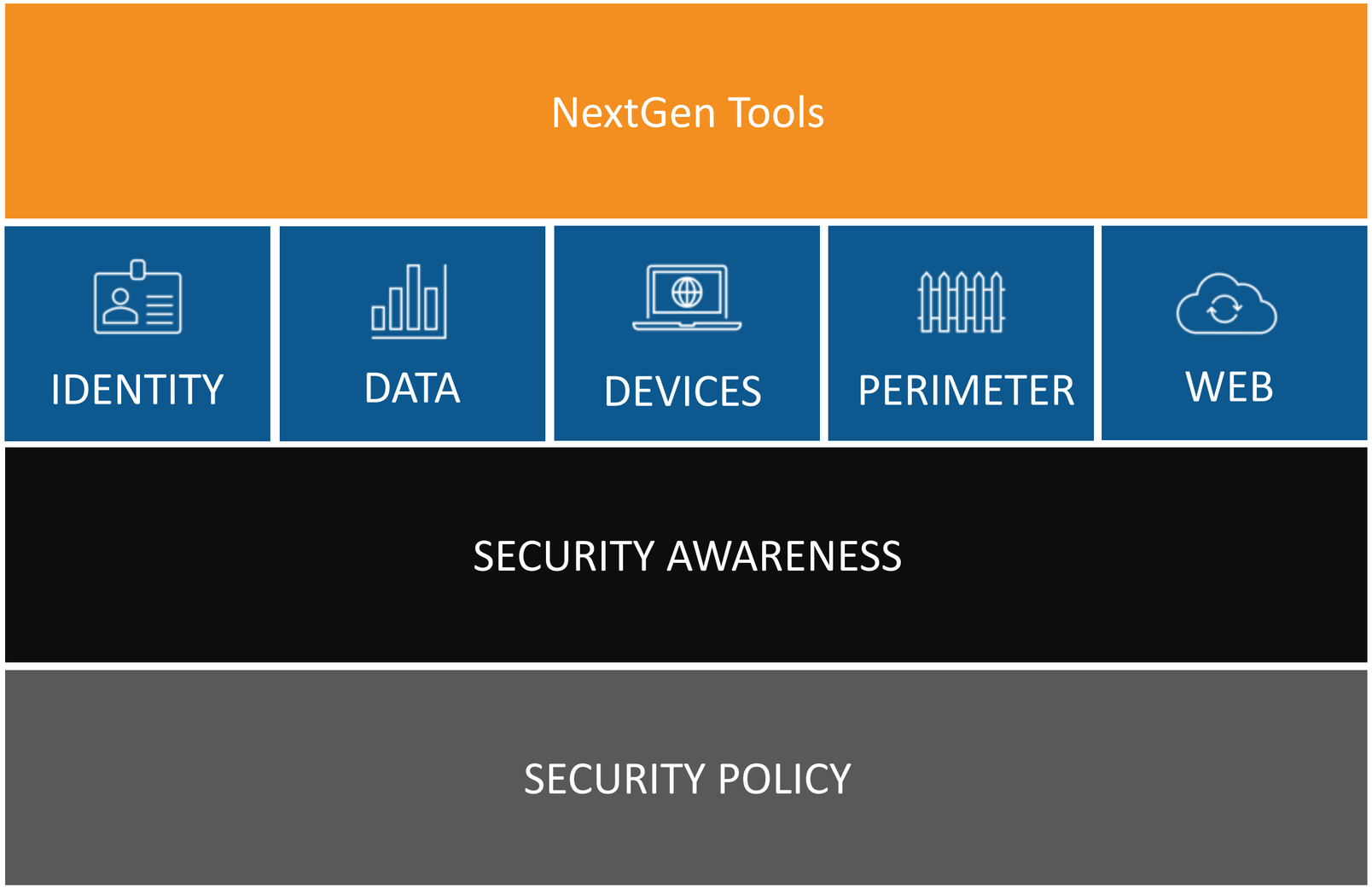


Genius Hacker – 197 IQ

CommunityIT Innovators® where technology meets mission

Cybersecurity - Adversaries

OUR APPROACH TO CYBERSECURITY

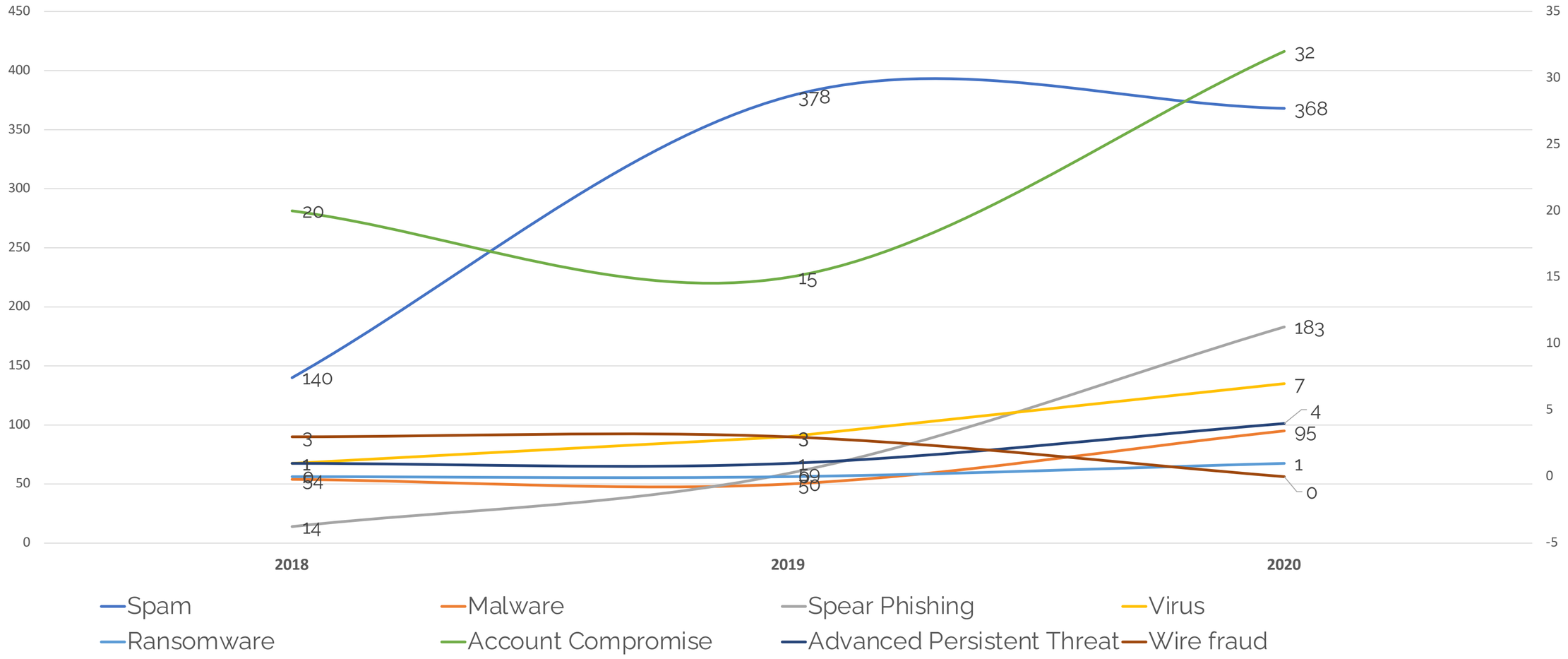


Poll #2

Have you experienced any of the following?

- Spam
- Phishing
- Account Compromise
- Malware
- Wire Fraud
- Virus
- Ransomware
- Advanced Persistent Threat

Nonprofit Cybersecurity Incidents



CYBERSECURITY LANDSCAPE

Does your nonprofit do any of the following?

- Process donations
- Process online event registrations
- Store personal information for program participants
- Collect information on donors or newsletter subscribers
- Initiate online vendor payments

If so…your entity is at risk for cybersecurity threats

2

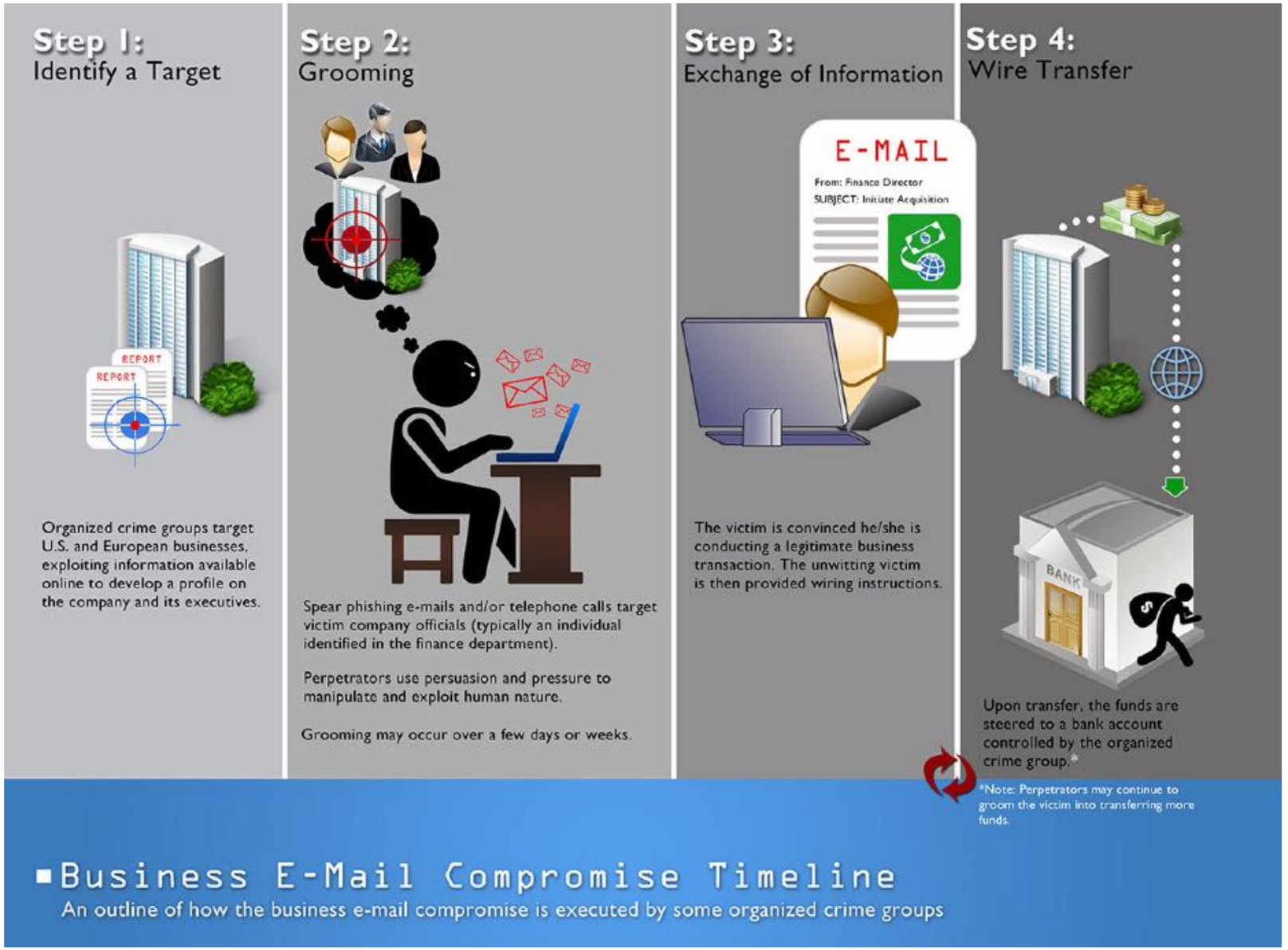
Types of Cybersecurity Incidents

Examples

CommunityIT Innovators® where technology meets mission

YOUR PART-TIME CONTROLLER®
The NONPROFIT accounting specialists™

Types of Cybersecurity Incidents



Types of Cybersecurity Incidents

Phishing Scam Case Nonprofit employees fell victim to fake business invoices

- Scammers targeted finance department employees
- Invoice appeared to come from an actual vendor
- Funds were sent via wire transfer so almost impossible to get back
- Employees lacked training on phishing schemes

Types of Cybersecurity Incidents

Phishing Scheme Example

-----Original Message-----
From: Tom [redacted] [mailto:tom.[redacted]@[redacted].com]
Sent: Wednesday, [redacted] 7:18 AM
To: Tim [redacted]
Subject: Fund Transfer

Tim,

I would like to know if you can process a wire transfer today? Let me know so I can send you the bank details.

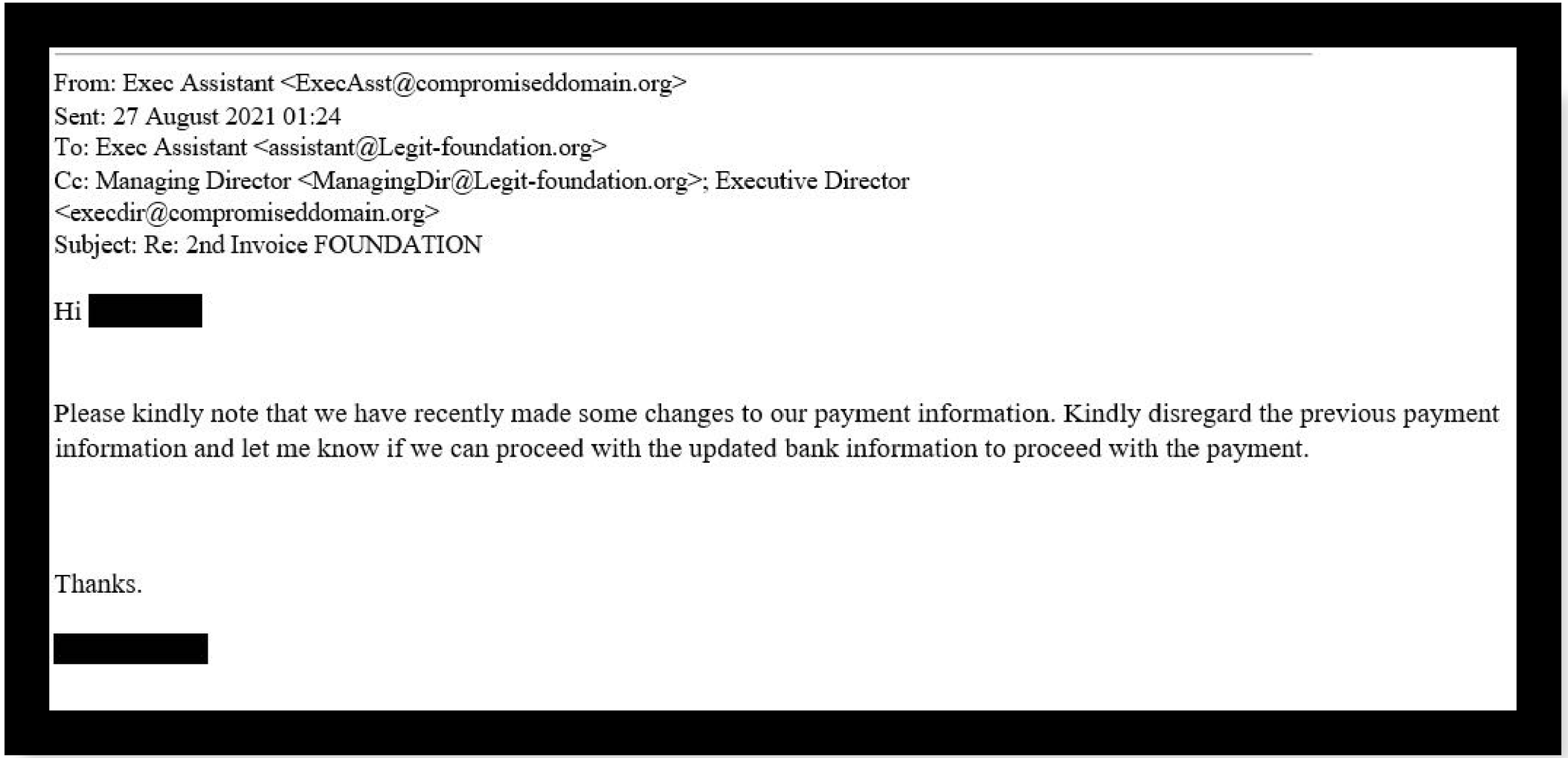
Regards,
Tom [redacted]

Types of Cybersecurity Incidents

Phishing Schemes

- How to detect and prevent
  - Promote an environment of **healthy skepticism**!
  - Do not click on links or respond to requests for money, bank account information, or credit card information
    - If the Executive Director really needed that wire transfer *today*, wouldn't he/she just pick up the phone or walk over to the A/P department and ask?
  - Take a closer look at the sender's email address
  - Hover over links to confirm their validity

Compromised account leads to Fraud



From: Exec Assistant <ExecAsst@compromiseddomain.org>
Sent: 27 August 2021 01:24
To: Exec Assistant <assistant@Legit-foundation.org>
Cc: Managing Director <ManagingDir@Legit-foundation.org>; Executive Director <execdir@compromiseddomain.org>
Subject: Re: 2nd Invoice FOUNDATION

Hi [redacted]

Please kindly note that we have recently made some changes to our payment information. Kindly disregard the previous payment information and let me know if we can proceed with the updated bank information to proceed with the payment.

Thanks.

[redacted]

Sophisticated Typo squatting Attack

Pick out the legitimate domain name

grameenkota.org	grameenkoota.org
idfcfirstbank.com	idfcfrstbank.com
phoenixlegal.nl	phoenixlegal.in

Sophisticated Typo squatting Attack

Pick out the legitimate domain name

grameenkota.org	**grameenkoota.org**
idfcfirstbank.com	idfcfrstbank.com
phoenixlegal.nl	**phoenixlegal.in**

Sophisticated Typo squatting Attack

From: Alhad Sardesai <alhad.sardesai@idfcfrstbank.com>
Sent: Wednesday, September 25, 2019
To: Manjunath D R <manjunath.dr@grameenkota.org>
Cc [redacted] Ranjini R <ranjini.r@gramenkoota.org>; Diwakar B R <diwakar@grameenkota.org>; Aditya Bhargava <aditya.bhargava@phoenixlegal.nl>; Chandrakanth S <chandrakanth.s@gramenkoota.org>;
Subject: RE: 2019 Loan Documents - [redacted] - Grameen Koota

Manjunath,
The previous bank account is unavailable to receive funds due to some technical Error. Please find the attached Alternative Trust Bank details in the attached.

Sorry for any inconveniences caused.

Regards
Alhad Sardesai
Director
Financial Markets Sales

3

Financial processes and IT tools

To help prevent and detect fraudulent activity

CommunityIT Innovators®
where technology meets mission

YOUR PART-TIME CONTROLLER®
The NONPROFIT accounting specialists™

Financial processes and IT tools

Let's face it – fraud happens!

- The best defense? **Heightened awareness!**

What are our tips to help protect your organization from fraud?

1. **Establish the proper tone from the top**
2. **Understand high risk areas**
3. **Establish and enforce policies and procedures**

Financial processes and IT tools

Establish the proper tone from the top

- The actions of your management and board set the example for the rest of the organization
- Provide ongoing fraud training for staff and board members
- Provide employees an anonymous avenue under which to report suspicious activity
  - "If you see something, say something"

Financial processes and IT tools

Understand high risk areas

Does your organization enforce segregation of duties for these areas?

- Cash disbursements such as:
  - Credit card transactions
  - Online bill payments
  - Checks
- Cash receipts
- Payroll

Financial processes and IT tools

Establish and enforce policies and procedures

- System controls over access to the accounting information system
- Policies and procedures for financial management
- Procedures for board involvement
  - Board meeting schedule and expected participation
  - Financial report review and monitoring of variances

Best Practices - Finance

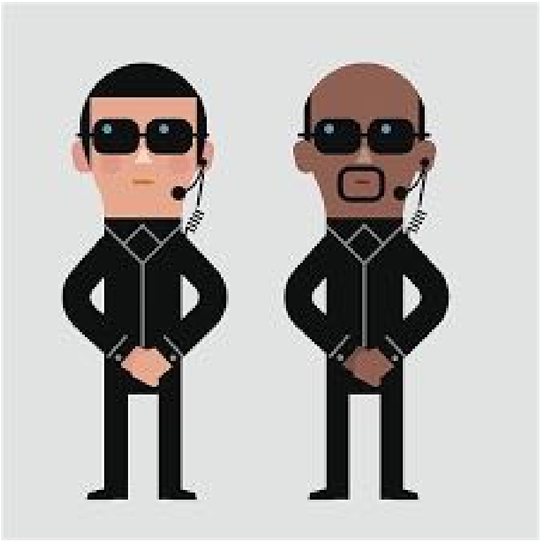
Through our work, we've collected some valuable tips to help clients in their security and fraud prevention efforts:

- Banking services that help prevent fraud
- Internal controls around cash disbursements and receipts
- Common sense considerations for internet safety

Best Practices - Finance

Call (bank) security!

- Banks offer many services that help customers with fraud prevention
- Banks typically charge for some services, but it's far less than the cost from fraudulent acts



Best Practices - Finance

Recommended internal controls around cash disbursements and receipts:

- Daily review of online banking activity
- Requiring a second signature on checks
- Limiting the use of company credit cards
  - We advise against the use of debit cards
- Utilizing electronic services such as
  - Remote deposit service
  - 2-step electronic payment process
  - Vendor payment sites

Best Practices- Technology

Security Awareness Training:

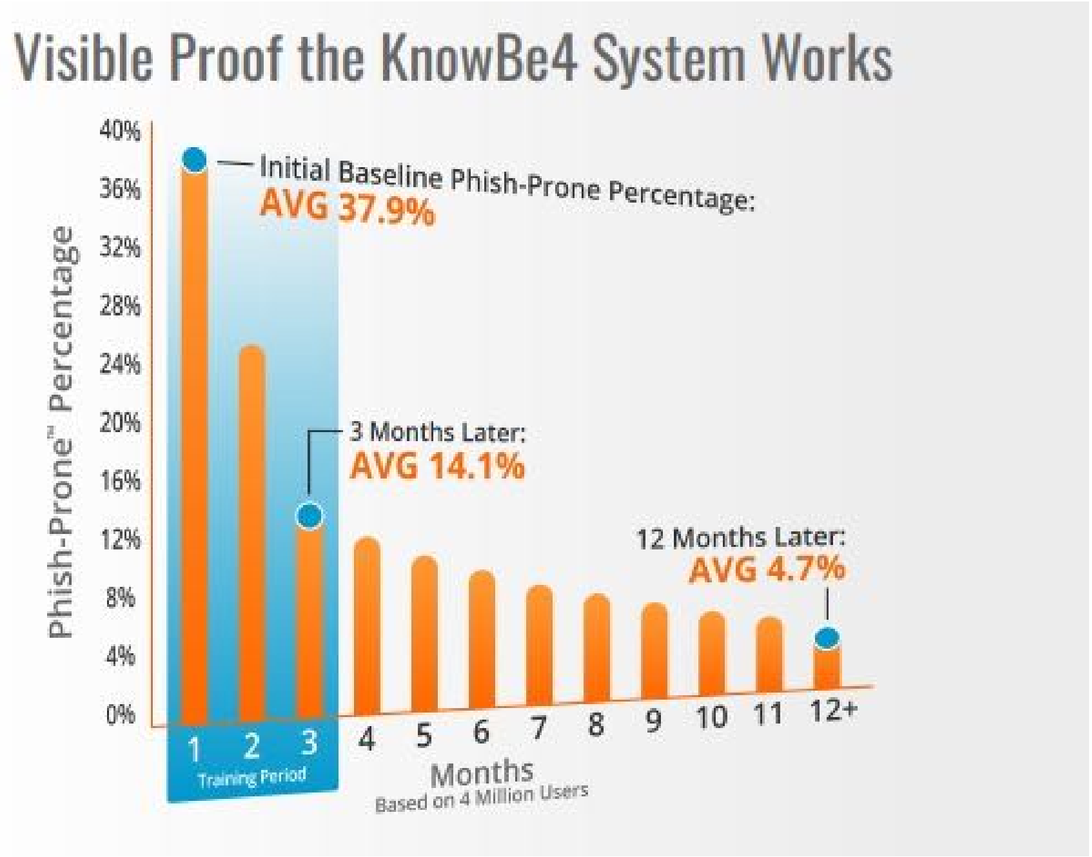
- Engaged and educated staff help avoid risk
- Mandatory for all staff and led from the top
- Weekly Micro-training or Monthly – Annual no longer adequate
- We see training as very effective

Best Practices- Technology

Cybersecurity Awareness

SMB Nonprofits (1-249 employees)

- Phase 1 (Initial baseline results) – **39.4%**
- Phase 2 (90 days after initial training) – **14.9%**
- Phase 3 (1 year into training program) – **4.8%**



Best Practices- Technology

MFA Enrollment

What does MFA stand for?

- MultiFactor Authentication and it requires something you know, your password, and something you have, your smartphone, to login

How will it affect me?

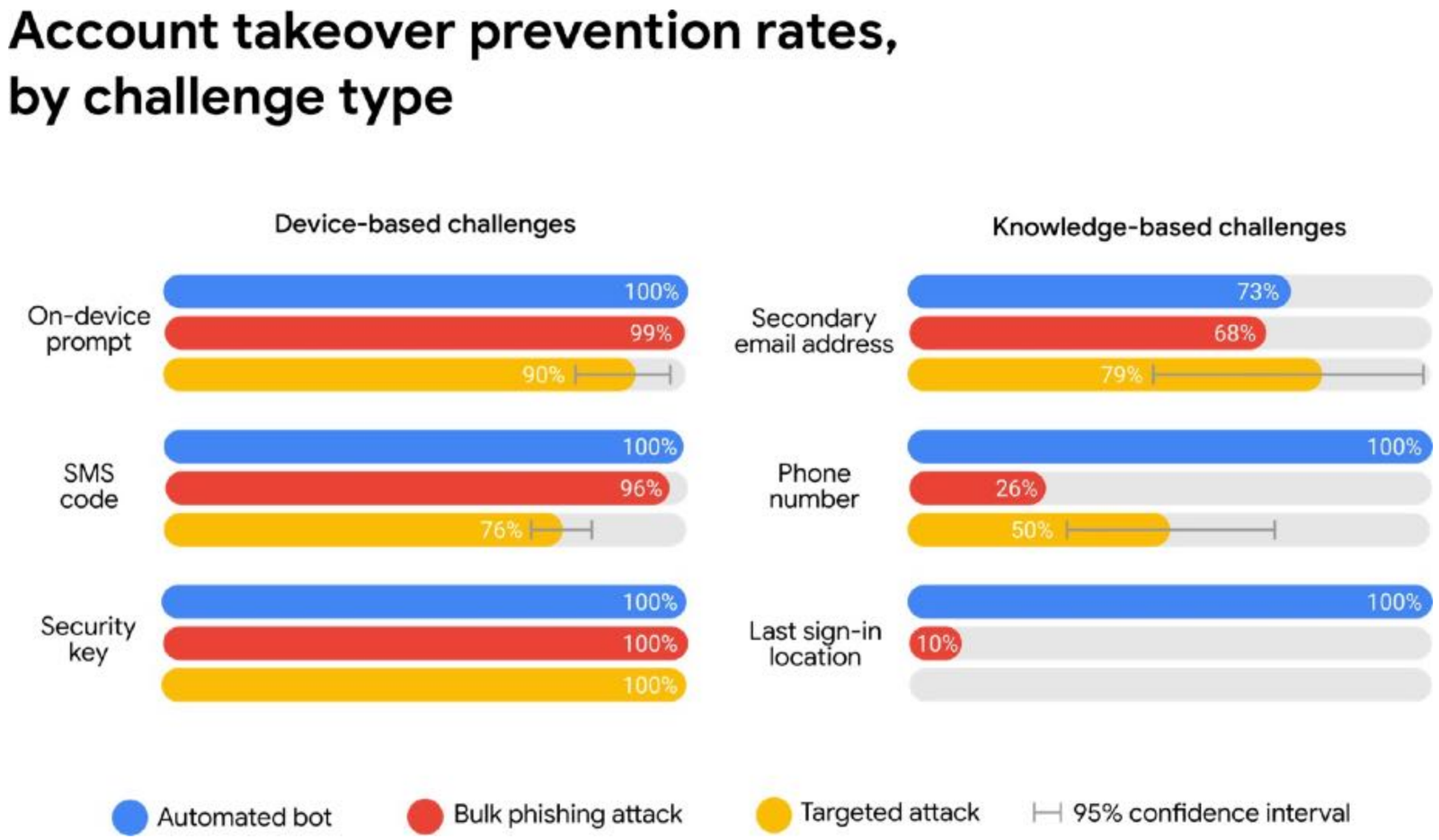
- You'll be required to enroll your account in MFA and setup an app on your smartphone.

Will it be a distraction for me?

- No. Staff will be prompted to confirm their login periodically. You may be prompted more if you travel. You shouldn't be prompted in the office.

Best Practices- Technology

MFA is Effective – Research from Google



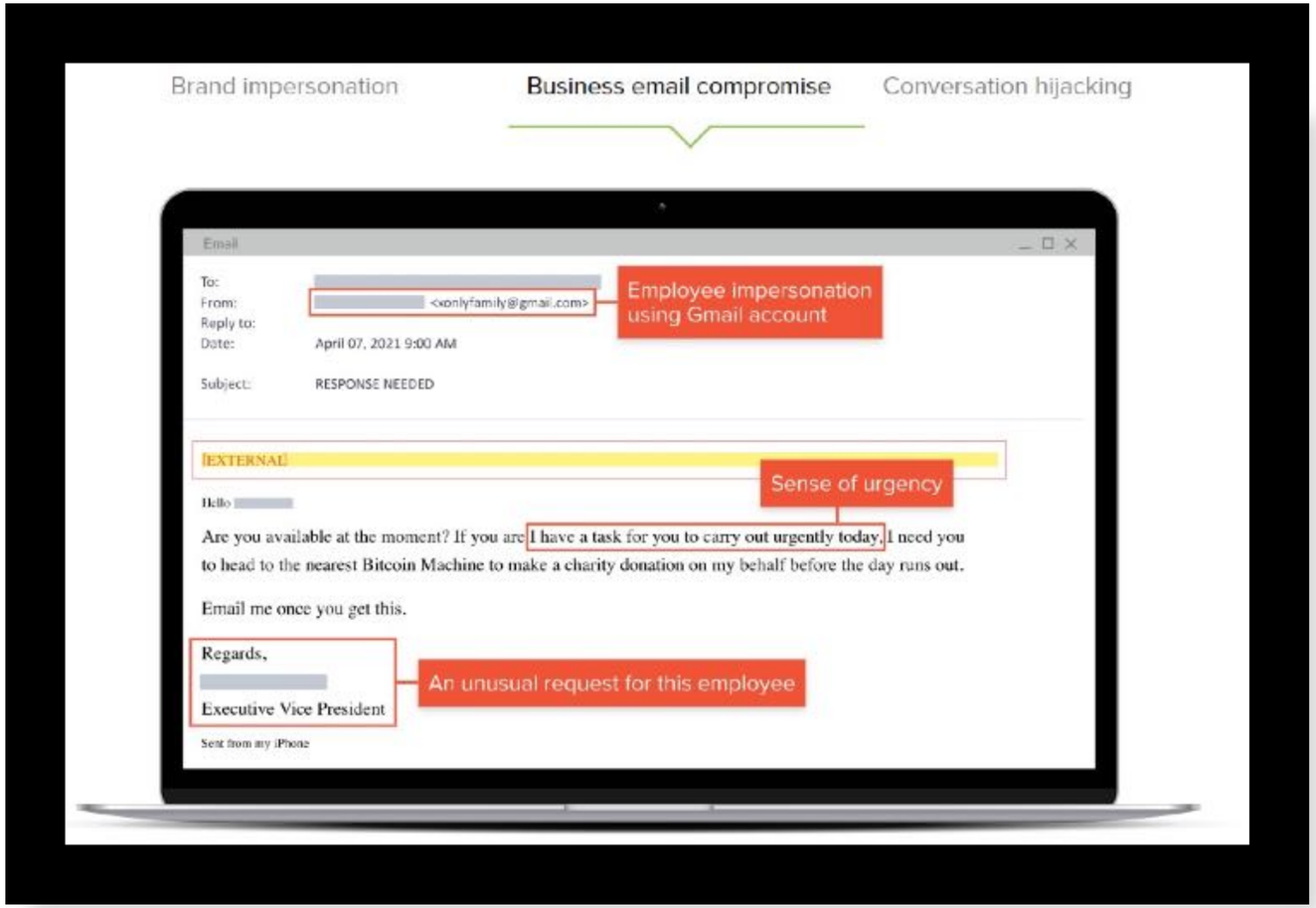
Best Practices- Technology

Advanced Email Protection

- New attacks require new protection
- Advanced email protection works differently
- Uses API integration to analyze email, activities and relationships
- Provides insight and analysis to IT Teams

Best Practices- Technology

Advanced Email Protection



Best Practices- Checklist

- **Establish baseline IT security controls**
  - Security Awareness Training
  - MFA
- **Define, and follow finance processes**
  - Set the tone from the top
  - Understand your organization's risk
  - Promote secure internal control environment
- **Layer on technology solutions**
  - Email protection
  - Endpoint detection and response

Questions?

YOUR PART-TIME CONTROLLER®
The NONPROFIT accounting specialists™

CommunityIT Innovators®

Upcoming Webinar

Diverse Perspectives on Thriving in Nonprofit Tech Careers

Wednesday March 16

3:00 pm EST, 12noon PST