



Practical, provocative,
food for thought for nonprofits



Cyber Security 101 for Nonprofits

Presented by:

Leda Muller

Achieving Excellence in Cyber Security for
All Nonprofits Through Education and Empowerment

Agenda

Information Technology vs Cyber Security

Why is cyber security important for nonprofits?

Tips for being more secure in your organization

Assessing your environment

Q&A

Achieving Excellence In Cyber Security For All Nonprofits Through Education and Empowerment



Information Technology

Cyber Security



Information technology focuses on the systems that store and transmit digital information.



Cyber Security focuses on protecting electronic information stored within those systems.

What is Cyber Security?

Why is Cyber Security important to nonprofits?

[CISA \(Cybersecurity Infrastructure Security Agency\)](#) states “Cyber security is the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information.”

Nonprofits both internally and externally are a source of sensitive data that if not managed properly can be exploited by cybercriminals at any moment.

Sensitive Data	External Sources Location
SSN, addresses, names, bank/credit card, passport info of nonprofit service users	Data hosted on websites on the Internet for donors, sponsors, nonprofit service users
Sensitive employee and medication info	Unsecured nonprofit websites publicly facing on the Internet

**4.24 million
US Dollars**



**Cybercrime increased 600%
over the past 2 years.**

A green fingerprint background with the text '90%' in the center.

90%

Recent Breaches of Nonprofits



2015

Utah Food Bank

**10,000 donors
info breached**

Names, address,
credit/debit card
information exposed.



2019

People Inc.

**Comprised email
account data breach**

Medical data of
end users exposed.



2020

Blackbaud

Ransomware attack

SSNs, passports, PHI,
financial information exposed.



2022

International Committee of the Red Cross

**Government sponsored
cyberattack**

515,000 people impacted, sensitive
data exposed due to an open security
risk that cybercriminals exploited.

Cybercriminals constantly look for holes to find a way in, much like a mouse!



In the Red Cross cyberattack...

The malware created for this attack was tailor-made for the ICRC's infrastructure and antivirus software.



American Red Cross

How to be more secure in your organization?

Password Management Best Practices


-  Unique passphrase passwords
purple*fox!is3amazing
-


Password Managers




-  Multi Factor Authentication Apps
Duo, Google Authenticator, Authenticator

Looking for Suspicious Indicators in Emails, Texts, & Phone Calls

-  Think before you click! Does the message make you worried? Cybercriminals know what makes you tick!

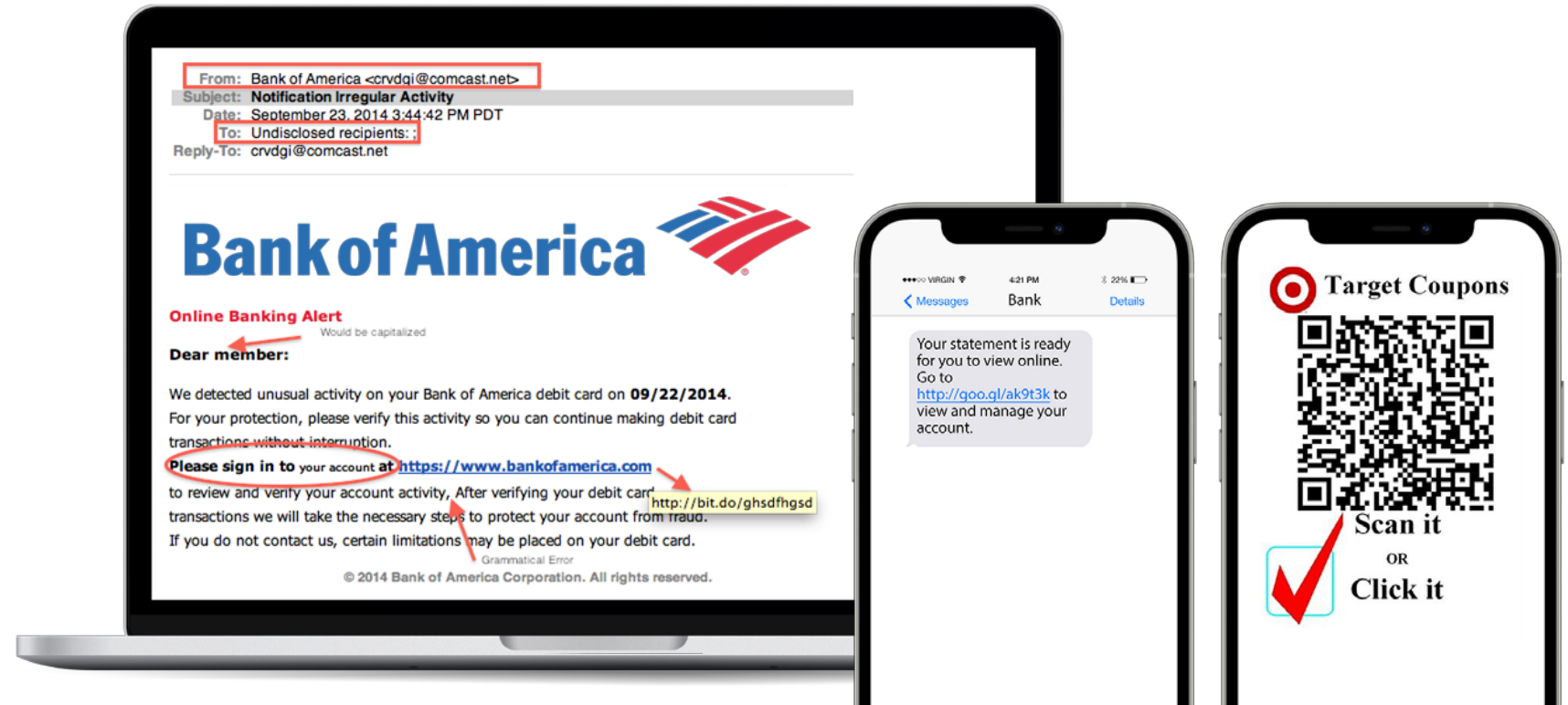
-  Hover over website links or hyperlinks in documents. Hyperlinks usually have underlines under text and may be highlighted in **blue**.

-  Is the message showing a sense of urgency?

How to spot suspicious activity?

What should I do if faced with a message I feel wary about?

- Let IT or your manager know
- Call/Text/Email the sender of the message and verify
- Report as Phishing or Spam in Gmail or Outlook where possible
- Avoid responding to texts, block if possible

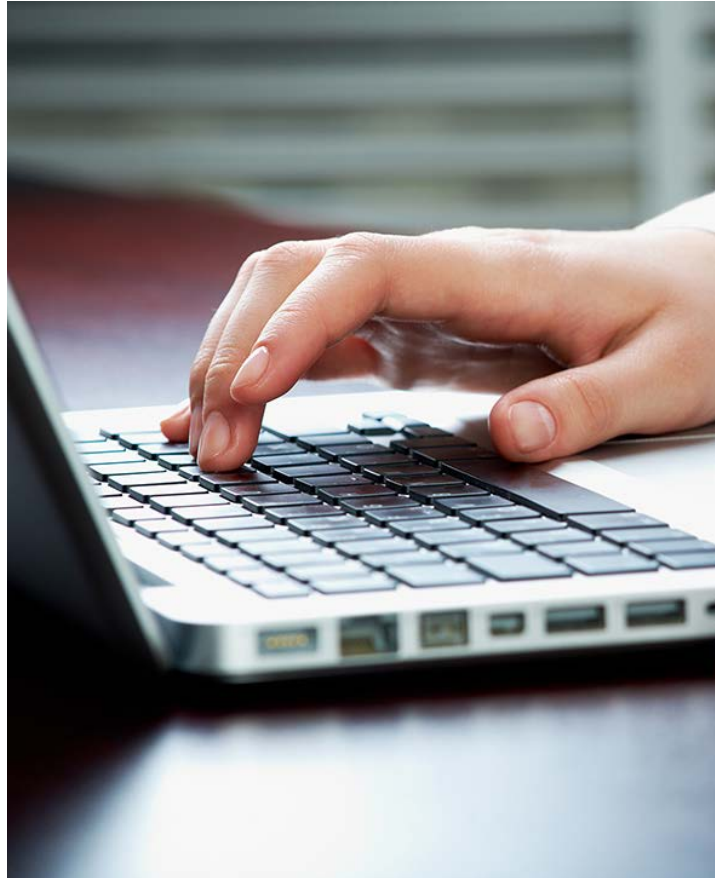


How can I be secure when working remotely?

Be cautious of oversharing on social media.

Work ID badges with new job posts, passports, vacation updates.

Beware of shoulder surfers.



Use Antivirus and keep routers updated.

Avoid using public WiFi for sensitive tasks.

Ex. personal data, banking, identity information.

Security Assessment

A comprehensive assessment that will identify potential vulnerabilities in your organization

Data: Classification

- Types of data

Inventory of Assets

- Technology
- Ownership

People

- Employees
- Volunteers
- BOD
- Donors

Access: Management

Systems

- Applications
- Servers

3rd Party Vendors

- Contracts
- Assessments



Think about your organization?

39 seconds

Hackers attack every 39 seconds.
(University of Maryland)

94%

of malware is delivered by email.
(Verizon)

56%

of nonprofits do not require multi factor authentication (MFA) to log into an online account. (NTEN)

Only 26%

of nonprofits actively monitor their environment. (NTEN)

59%

of nonprofits do not provide cybersecurity training to their staff on a regular basis. (NTEN)

Only 20%

of nonprofits have a policy in place to address cyberattacks. (NTEN)

More than 70%

of nonprofits have not run even one vulnerability assessment to evaluate their potential risk exposure. (Cohn Reznick)

Q & A

How to get information about Pocket Security?

[Reach us via https://pocketsecurity.org/contact-us](https://pocketsecurity.org/contact-us)



Thank You

blue[®] avocado

Practical, provocative,
food for thought for nonprofits

blueavocado.org

Offer for Blue Avocado Subscribers

<https://confidently.com/>

1. **Sign up yourself** for a free Confidently personal account at www.confidently.com
 - Use coupon code BLUEAVOCADO at check-out to get your free 90-day trial
2. We'll follow up with you directly to **schedule a demo of the Confidently enterprise service**
 - Includes individual employee dashboards, an enterprise-wide dashboard, alerts, configuration panel, and bulk enrollment to manage Confidently across your organization, reduce overall attack surface, and gain threat intelligence
3. **Sign up ~10 employees for a free enterprise pilot** of Confidently's data privacy service
4. After successful pilot, **roll out Confidently service to broader set of employees** (and/or donors, members, and supporters) for just \$10/month/user

Contact brent@confidently.com with any questions