



Cybersecurity Awareness

Current Scams

&

The Need for an Awareness Program



Donald E. Hester

- Email: DonaldH@MazeAssociates.com
- Phone: (925) 930-0902
- Blog: www.LearnSecurity.org
- Twitter: [@sobca](https://twitter.com/sobca)
- Webinars: www.brighttalk.com/channel/17235
- mazeassociates.com/cybersecurity/



The Bad Guys



Insider Threats



Cyber Activists



Cyber Criminals



Nation States



Cryptojacking



Collateral Damage



Destruction



Ransom



Data Theft



All of the Above

Atlanta

CNN U.S. + Live TV U.S. Edition

The FBI is investigating a ransomware attack on the city of Atlanta

By **Emanuela Grinberg**, CNN
Updated 9:35 AM ET, Fri March 23, 2018

WGCL

Mayor Keisha L
Atlanta

0:04 / 1:06

BUSINESS > TECHNOLOGY

Cyberattacks, like the one on CDOT, a wakeup call for local governments to prepare

After two attacks Colorado transportation department sped up

Technically | Baltimore News Jobs Events Subscribe

CIVIC
Mar. 29, 2018 12:42 pm

City: Cyber attack against Baltimore's 911 computer-aided dispatch system was ransomware

Atlanta's Ransomware Cleanup Costs Hit \$2.6 Million

Money Would Have Been Better Spent on Prevention, Experts Say

Mathew J. Schwartz (@euroinfosec) · April 24, 2018 0 Comments

government technology


SECURITY

Local Governments: Attractive Targets for Cybercriminals?

Cities and counties are attractive targets in part because they're connected to state systems or other large networks.

BY ANDY MATARRESE, THE COLUMBIAN, VANCOUVER, WASH. / MAY 4, 2016

the past year



Get the ITPro Newsletter

Get FREE weekly newsletters from ITPro - delivering the latest news, reviews, insight and case studies.

[Click here](#)

CNN U.S. + Live TV U.S. Edition +

The FBI is investigating a ransomware attack on the city of Atlanta

By Emanuela Grinberg, CNN Updated 9:35 AM ET, Fri M

Mayor Keisha L Atlanta

0:04 / 1:06

BUSINESS > TECHNOLOGY

Cyberattacks, like the one on CDOT, a wakeup call for local governments to prepare

Technically | Baltimore News Jobs Events Subscribe

Mar. 29, 2018 12:42 pm

City: Cyber attack against Baltimore's 911 computer-aided dispatch system was

Cybercrime as-a-service , Data Breach , Fraud Management & Cybercrime

Atlanta's Reported Ransomware Bill: Up to \$17 Million

City Didn't Pay Ransom, But Spends for Cleanup, New Devices, Better Security

Mathew J. Schwartz (@euroinfosec) · August 6, 2018 0 Comments

SECURITY

Local Governments: Attractive Targets for Cybercriminals?

Cities and counties are attractive targets in part because they're connected to state systems or other large networks.

BY ANDY MATARRESE, THE COLUMBIAN, VANCOUVER, WASH. / MAY 4, 2016



Get the IPro Newsletter

Get FREE weekly newsletters from IPro - delivering the latest news, reviews, insight and case studies.

Click here



Baltimore

CNN U.S. + Live TV U.S. Edition +
The FBI is investigating a ransomware attack on the city of Atlanta

BUSINESS > TECHNOLOGY
Cyberattacks, like the one on CDOT, a wakeup call for local governments to

Technically | Baltimore News Jobs Events Subscribe
CIVIC
Mar. 29, 2018 12:42 pm
City: Cyber attack against Baltimore's 911

Cybercrime as-a-service , Endpoint Security , Fraud Management & Cybercrime

Baltimore Ransomware Attack Costing City \$18 Million

City's IT Department Continuing Recovery Work

Scott Ferguson (@Ferguson_Writes) · June 7, 2019

SECURITY
Local Governments: Attractive Targets for Cybercriminals?
Cities and counties are attractive targets in part because they're connected to state systems or other large networks.
BY ANDY MATARRESE, THE COLUMBIAN, VANCOUVER, WASH. / MAY 4, 2016



Get the ITPro Newsletter
Get FREE weekly newsletters from ITPro - delivering the latest news, reviews, insight and case studies.
[Click here](#)



RECOMMENDED

How 'Joe Exotic' went from a presidential run to prison

'A mother's worst nightmare': Frantic search for missing Hawaii hiker extends into fifth day

Here's what's happening in the week ahead

Improbable 'looking good' in breeze for Preakness

Tyra Banks creating an amusement park in Los Angeles

Escalating US-China trade war sends stocks plunging

Six days later, Baltimore government is still recovering from ransomware attack

Share [Facebook] [Twitter] [Link]



Updated: 5:15 PM EDT May 13, 2019

Lowell Melser [Facebook] [Twitter] [Email]
News Reporter, Meteorologist



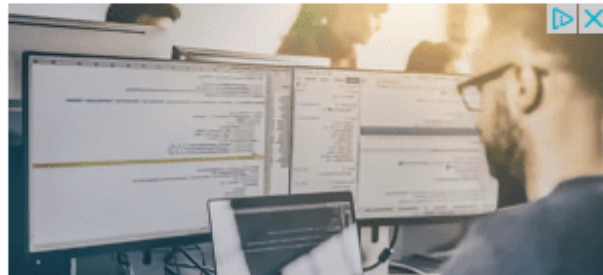


Baltimore finance director says people who paid taxes at last minute won't be penalized because of ransomware



By **Ian Duncan** • **Contact Reporter**
The Baltimore Sun

MAY 13, 2019, 1:55 PM





Data Breaches

Breach Notification , Cybercrime , Fraud Management & Cybercrime

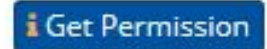
Report: LAPD Data Breach Exposes 2,500 Officer Records

Police Database Includes Email Addresses and Partial Social Security Number

Akshaya Asokan ([@asokan_akshaya](#)) · July 30, 2019



Credit Eligible



<https://www.govinfosecurity.com/report-lapd-data-breach-exposes-2500-officer-records-a-12856>



Email compromise hits \$12 Billion in costs



Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION



Jul 12, 2018

Alert Number
I-071218-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office**.

Local Field Office Locations:
www.fbi.gov/contact-us/field

BUSINESS E-MAIL COMPROMISE THE 12 BILLION DOLLAR SCAM

This Public Service Announcement (PSA) is an update and companion to Business E-mail Compromise (BEC) PSA 1-050417-PSA posted on www.ic3.gov. This PSA includes new Internet Crime Complaint Center (IC3) complaint information and updated statistical data for the time frame October 2013 to May 2018.

DEFINITION

Business E-mail Compromise (BEC)/E-mail Account Compromise (EAC) is a sophisticated scam targeting both businesses and individuals performing wire transfer payments.

<https://www.ic3.gov/media/2018/180712.aspx>



CEO Fraud is a type of business email compromise.

It does not mean the CEO is committing fraud.

It means someone impersonates the CEO and makes a request of staff.

Tech Giants Fall Victim to \$100 Million CEO Fraud

- The scammer, a 48-year old Lithuanian managed to trick these two technology companies into wiring him \$100 million.
- This scam surfaced as the U.S. government filed a civil forfeiture lawsuit in federal court in Manhattan seeking to recover tens of millions held in at least 20 bank accounts around the world.



Google and Facebook Were Victims of a \$100 Million Scam
Proving no one is immune to phishing.

Turns out even the most powerful tech companies aren't immune to phishing scams

<http://fortune.com/2017/04/27/facebook-google-rimasauskas/>



Cybercriminals targeting employee usernames and passwords



Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION



Sep 18, 2018

Alert Number
I-091818-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office**.

Local Field Office Locations:
www.fbi.gov/contact-us/field

CYBERCRIMINALS UTILIZE SOCIAL ENGINEERING TECHNIQUES TO OBTAIN EMPLOYEE CREDENTIALS TO CONDUCT PAYROLL DIVERSION

The IC3 has received complaints reporting cybercriminals are targeting the online payroll accounts of employees in a variety of industries. Institutions most affected are education, healthcare, and commercial airway transportation.

METHODOLOGIES

Cybercriminals target employees through phishing emails designed to capture an employee's login credentials. Once the cybercriminal has obtained an employee's credentials, the credentials are used to access the employee's

<https://www.ic3.gov/media/2018/180918.aspx>



Tech support fraud on the rise



Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION



March 28, 2018

Alert Number
I-032818-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office**.

Local Field Office Locations:
www.fbi.gov/contact-us/field

TECH SUPPORT FRAUD

Based on new reporting, the Internet Crime Complaint Center (IC3) is providing updated guidance regarding technical support fraud. Tech Support Fraud involves a criminal claiming to provide customer, security, or technical support in an effort to defraud unwitting individuals. This type of fraud continues to be a problematic and widespread scam.

In 2017, the IC3 received approximately 11,000 complaints related to tech support fraud. The claimed losses amounted to nearly \$15 million, which represented an 86% increase in losses from 2016. While a majority of tech support fraud involves victims in the United States, IC3 has received complaints from victims in 85 different countries.

Criminals may pose as a security, customer, or technical support representative offering to resolve such issues as a compromised e-mail or bank account, a virus on a computer, or to assist with a software license.



Increase in W-2 scams



Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION



February 21, 2018

Alert Number
I-022118-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office**.

Local Field Office Locations:
www.fbi.gov/contact-us/field

INCREASE IN W-2 PHISHING CAMPAIGNS

Beginning in January 2017, IRS's Online Fraud Detection & Prevention (OFDP), which monitors for suspected IRS-related phishing emails, observed an increase in reports of compromised or spoofed emails requesting W-2 information. Sometimes these requests were followed by or combined with a request for an unauthorized wire transfer.

The most popular method remains impersonating an executive, either through a compromised or spoofed email in order to obtain W-2 information from a Human Resource (HR) professional within the same organization.

Individual taxpayers may also be the targeted, but criminals have evolved their tactics to focus on mass data thefts.

<https://www.ic3.gov/media/2018/180221.aspx>

Business Email Compromise Schemes: Most Seek Wire Transfers

'CEO Fraud' Social Engineering Attacks Continue to Surge

Mathew J. Schwartz (@euroinfosec) • September 3, 2018 1 Comment




Credit Eligible

Get Permission



<https://www.databreachtoday.com/business-email-compromise-schemes-most-seek-wire-transfers-a-11452>



Home » Cybersecurity » Social Engineering » Business Email Compromise Continues to Plague

Business Email Compromise Continues to Plague



by Christopher Burgess on July 30, 2019

It seems that an annual jaunt through the success cybercriminals are having with business email compromise (BEC) and fleecing money from companies, organizations and governmental entities is a requirement. Last year we asked the question, “Are you vulnerable to BEC fraud?” defining BEC and sharing with you the activities of the FBI to thwart the cybercriminals. The key takeaway in 2018 was that cybercriminals were targeting individuals with fiscal authority. And, based on information released from the Department of Treasury, the criminals were having a well-paid field day. Things have changed a bit as we write this in July 2019.

Now we learn from the Financial Crimes Enforcement Network (FinCEN) the criminals continue to be extraordinarily well-paid. We also learn that the manufacturing and construction sectors are the top targets for business email compromise, according to the July 2019 “Financial Trends Analysis.”

The Financial Crimes Enforcement Network (FinCEN) reports that criminals continue to be extraordinarily well-paid.

<https://securityboulevard.com/2019/07/business-email-compromise-continues-to-plague/>



New Scams

- Spoof Phone Number
- Says they are from fraud prevention
- Will ask for CVV and PIN



The screenshot shows the top of a web page for KIMKOMANDO™, America's Digital Goddess. It features a navigation bar with a home icon, a yellow shopping cart icon labeled 'Shop', and a link to 'The Show'. Below the navigation bar is a white article header with the date 'October 4, 2018' on the left and a 'Leave a comment' button with the number '4' on the right. The main headline reads 'New clever bank phishing scam is spreading and it's duping even the experts'. The byline below the headline is 'By Francis Navarro, Komando.com'.

<https://www.komando.com/happening-now/494919/new-clever-bank-phishing-scam-is-spreading-and-its-duping-even-the-experts>



ACH / Direct Deposit



Blog

Webinars

Classes

Contributors

Social

Contact Us

Search

BrightTALK

Cybersafety

Crime

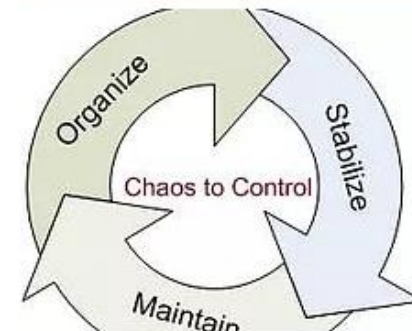
New Scams April 2019

8 Apr 2019 | Donald E Hester

ACH Scam

Vendor ACH request fraud is on the rise. The scam works this way, cybercriminals stalk their prey (research or intelligence gathering) looking for a new contract award for a vendor or find an existing vendor typically for a local government. Information

Featured Posts



Chaos to Control

<http://www.learnsecurity.org/single-post/2019/04/08/New-Scams-April-2019>



Gift Card Scams

The screenshot shows the top navigation bar of the Apple Support website with links for Mac, iPad, iPhone, Watch, TV, Music, and Support. The main content area features the heading 'Support' and 'About Gift Card Scams'. Below the heading, there is a warning: 'Be aware of scams involving App Store & iTunes Gift Cards and Apple Store Gift Cards.' A paragraph of italicized text provides instructions: 'If you believe you're the victim of a scam involving App Store & iTunes Gift Cards or Apple Store Gift Cards, you can call Apple at [800-275-2273](tel:800-275-2273) (U.S.) and say "gift cards" when prompted.' The bottom of the screenshot shows the start of another paragraph: 'A string of scams are taking place asking people to make payments over the phone for things such as'.

<https://support.apple.com/itunes-gift-card-scams>



Government Imposter Scams

- Calls or emails
- Claim to be from FBI, Social Security, IRS, Medicare, Local PD
- Use fear of authority and consequences
- Convey a sense urgency
- Often ask for payment by gift card or wire transfer



What to do?

- Don't trust caller ID, the number can be spoofed.
- Check with the real agency.
- Never pay with a gift card or wire transfer.
- Report government imposters scams at [ftc.gov/complaint](https://www.ftc.gov/complaint)



Scamming Positive Pay

- Altering the Payee on a check
- Positive Pay only checks the amount and check number
- Automated systems can recognize the check number and amount
- Automated systems don't check the payee



Is Employee Security Training Worth It?

IT pros have mixed feelings on how effective employee training initiatives are in improving their company's overall security posture. While employee security training can be a cost-effective way to improve awareness, it does lack some of the scalability and automation of other technical-based solutions.

Nicole Henderson | Oct 16, 2018

“Research from Spiceworks has found that employee training tools are one of the most effective ways for smaller businesses to improve security, especially from a cost perspective.”

<https://www.itprotoday.com/network-security/employee-security-training-worth-it>



Employees May Seek Treble Damages From NC Employer In Class Action Over Phishing Scam

5.16.2018

J.M. Durnovich

By now, you've surely been warned of so-called "phishing" e-mails. The failure to heed such warnings may become more costly for North Carolina employers. According to a recent federal court decision, an employee who is tricked into sharing personal information in response to a phishing e-mail can be seen as committing an *intentional* disclosure under North Carolina's Identity Theft Protection Act. As a result, the employer could face *treble* damages for the employee's mistake.

Sophisticated Phishing Schemes

“According to a recent federal court decision, an employee who is tricked into sharing personal information in response to a phishing e-mail can be seen as committing an intentional disclosure under North Carolina’s Identity Theft Protection Act. As a result, the employer could face treble damages for the employee’s mistake.”



Maturity and Risk

Spectrum of Cybersecurity Awareness Programs



0

1

2

3

4

5

COBIT

Non-Existent

Initial

Repeatable

Defined

Managed

Optimized

SANS

Nonexistent

Compliance-Focused

Promoting Awareness & Behavior Change

Long-Term Sustainment & Culture Change

Metrics Framework

Risk

High

High/Moderate

Moderate

Moderate/Low

Low



The Facts



- According to the Verizon 2018 Data Breach Report, 93% of data breaches are linked to phishing or social engineering.

<https://www.verizonenterprise.com/verizon-insights-lab/dbir/>



Social Engineering

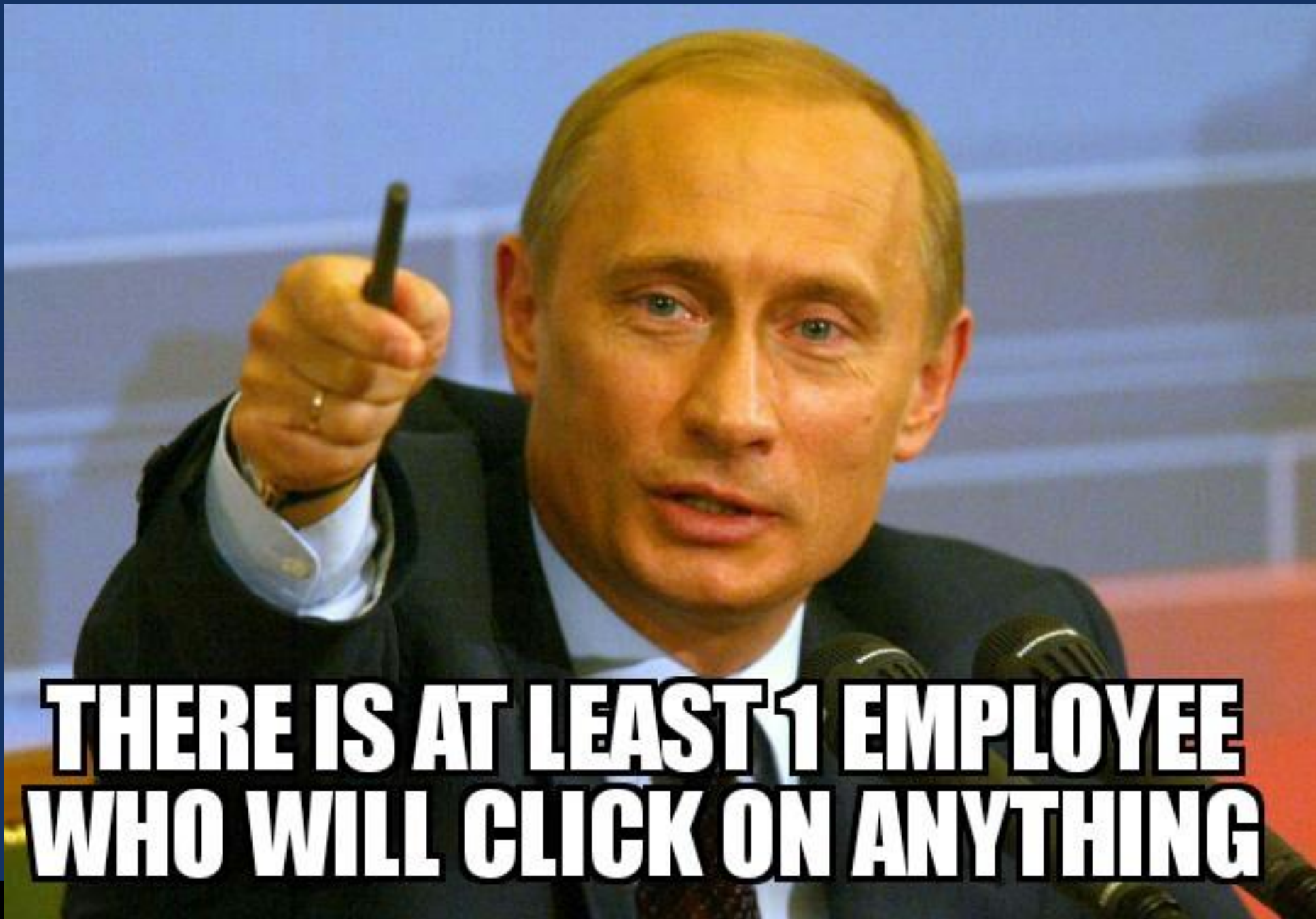


Phishing

Vishing

Spear Phishing

Whaling



**THERE IS AT LEAST 1 EMPLOYEE
WHO WILL CLICK ON ANYTHING**



Hackers know if they can get past you, they can get in.



People are the first and last line of defense for your
organization.

Do not leave your staff defenseless.



Awareness lowers 'cyber stress'

 TechRepublic.



SECURITY

Why improved cybersecurity education can help reduce employee 'cyber stress'

More than 80% of Americans said they were routinely stressed out by news of cyber attacks. Here's how to help.

By Jonathan Greig | May 1, 2018, 11:20 AM PST





Cybersecurity Awareness & Training

- Training
- Build Skills
- Roles based
- Awareness
- Reminders
- Curb risky behaviors





Cybersecurity Awareness Program

DRAFT NIST SP 800-53, REVISION 5

SECURITY AND PRIVACY CONTROLS FOR INFORMATION SYSTEMS AND ORGANIZATIONS

TABLE E-2: AWARENESS AND TRAINING FAMILY

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	WITHDRAWN	PRIVACY-RELATED	IMPLEMENTED BY	ASSURANCE	CONTROL BASELINES		
						LOW	MOD	HIGH
AT-1	Awareness and Training Policy and Procedures		P	O	A	X	X	X
AT-2	Awareness Training		P	O	A	X	X	X
AT-2(1)	PRACTICAL EXERCISES		P	O	A			
AT-2(2)	INSIDER THREAT			O	A	X	X	X
AT-2(3)	SOCIAL ENGINEERING AND MINING			O	A		X	X
AT-3	Role-Based Training		P	O	A	X	X	X
AT-3(1)	ENVIRONMENTAL CONTROLS			O	A			
AT-3(2)	PHYSICAL SECURITY CONTROLS			O	A			
AT-3(3)	PRACTICAL EXERCISES		P	O	A			
AT-3(4)	SUSPICIOUS COMMUNICATIONS AND ANOMALOUS SYSTEM BEHAVIOR			O	A			
AT-3(5)	PERSONALLY IDENTIFIABLE INFORMATION PROCESSING		P	O	A			
AT-4	Training Records		P	O	A	X	X	X
AT-5	Contacts with Security Groups and Associations	w	Incorporated into PM-15.					

Note: Privacy-related controls and control enhancements are not allocated to baselines in this table. See [Appendix F](#) for control selection and implementation guidance.

NIST SP 800-53 & 800-50

COMPUTER SECURITY RESOURCE CENTER



PUBLICATIONS

SP 800-50

Building an Information Technology Security Awareness and Training Program



Documentation

Topics

Date Published: October 2003



What to do?

- Start a program
- Train staff (At time of hire and ongoing)
- Test your staff (see improvement over time)
- Adjust as necessary
- Continuous improvement
- Lower cyber risk



Email Updates

Scam of the Week: Think Before You Tweet

If you've ever used social media to make a complaint about a company, you'd know that many organizations are quick to respond to this public expression. But have you ever stopped to question whether the account responding to your concern is really someone from the company?

Recently, fraudsters have taken to social media platforms to trick people into falling for their "help" and giving away their personal information. For example, a woman was upset with her broadband services so she took to Twitter to complain about her provider. She promptly received a response from an account appearing to be the customer service team for this company. The "customer service team" was able to gain personal information, and even banking information from her by using lines like: "I'm having trouble locating your account" and "I'll first need to ask you a security question". The woman soon found her bank account emptied out and several loans taken out under her name.

Clearly, this customer service team wasn't helping anyone aside from themselves.

Remember the following to protect yourself:

- Never trust that an account is legitimate based on their Twitter "handle", or any other "name" on social media. Just because the company name is present, doesn't make it valid.
- A legitimate organization would never ask you for sensitive data like your bank account information. If it sounds like a strange request, then it probably is.
- If you're having trouble with a product or service, log in to your account or reach out to their customer support channels, yourself. Never trust a response you receive after making a public complaint on social media or anywhere else online.



Ongoing

- Flyers
- Poster
- Social Media
- Infographics
- Ongoing Awareness



It will **NEVER** happen to me (says everyone it always happens to).



Scammers don't just target big organisations. If someone notifies you of a change in bank details, call & verify **BEFORE** making the payment.

watch A Goliath Hack for more info



STANDUPS 4

SECURITY

3 min A Goliath Hack



Popcorn Training



Metrics

Phishing Security Tests 12/17/2018 – 06/17/2019

26 Clicks 0 Replies 5 Attachment Open 0 Macro Enabled 0 Data Entered 967 Reported





Evaluating Emails

- Context
- Does the email ask for action
- Fear and urgency
- Selling
- Email address
- Links in the email
- Reach out - authenticate



Context

- What is the context of the email?
- Would this person/company be contacting me?
- Do I have business with them?
- Do I use this email with this organization/person?



Call to Action

- Is the email asking you to act on something in the email like click a link, open a file or call a number in the email?
- What is the email asking you to do?
- Is it a reasonable request?



Fear and Urgency

- Does the email appeal to fear?
- Does the email appeal for urgency?
- Does the email plead for compassion?
- Does the email claim an authority?



Selling

- Marketing people use some of the same tactics as cybercriminals
- Is the email selling something?
- If it is it is most likely SPAM
- Still don't click on it



Domain Names

- Ownership of a domain and sub domains
- What do you register ownership of?
- Domain MazeAssociates.com (last right dot)
- Subdomain Support.MazeAssociates.com
- Domain Link MazeAssocaites.com/cybersecurity
- Look for the dots “.” and the “/”



Evaluate the email address

- help@apple.com
- help@support.apple.com
- help@apple.net
- help@comcast.net
- help@app1e.com
- help@supportapple.com
- help@support-apple.com
- help@apple.support.com



Links in Email

- Are there links in the email?
- Do the links go to the correct address?
- Not perfect
- Marketers use tracking URLs
- Advance malware can change the URL in emails
- <https://protect-us.mimecast.com/...>



Reach Out

- Can you contact the person without using any contact information that is provided in the email?
- Should I authenticate this email or request?
(Confirm the identity of the sender.)
- Log into the website directly not using links from the email
- Contact the person – phone or email not using the contact information in the email



**We can help make the
world cybersafe!**

Cybersecurity Services

