Developing and Implementing an Effective Security Awareness Program

PEDRO SERRANO, CISSP
President ISSA-OK

OUR AGENDA

- PHISHING: HOW RANSOMWARE AND MALWARE GET DELIVERED
- BUT I HAVE A NEW $100,000 FIREWALL
- WHY IS SECURITY AWARENESS THE NEW SEXY
- WE EMPHASIZED ON CHANGING BEHAVIOR
- MONTHLY NEWSLETTERS ... ONE PAGE, NO ATTACHEMENTS
- MAKE REPORTING SUSPICIOUS EMAIL EASY
- BRIBE WITH FOOD
- CREATE “COMPETITION” OUT OF THE PHISHING CAMPAINS
- MADE TRAINING FUN, ANIMATED, EASY GOING

PHISHING

How ransomware and malware get delivered

Phishing is the number one vector for ransomware and malware to be delivered today

HOW MANY EMAIL ARE SENT AND RECEIVED

In 2016 this was 215.3 billion emails sent and received per day!
In 2017 this was 269 billion emails sent and received per day!
In 2018 this was 281.1 billion emails sent and received per day!

THE AVERAGE OFFICE WORKER RECEIVES 121 EMAILS A DAY

Email is the communication link for may companies ... In many instances depending on who send the email your sense of urgency sky rockets!

85% ORGANIZATION HAVE SUFFERED PHISHING ATTACK

This has become the new normal ...its not “IF but “WHEN”
This is critical when we can trace 90% of all malware started with an email

65% of all email users worldwide get their email via mobile device

I think this a very conservative figure ... “who does not get email in their phones?”
Prediction – This is going to be the new target of opportunity !!!!

THE DELIVERY

WHY THIS IS IMPORTANT?

BUT I HAVE A NEW FIREWALL

Your new $100,000 Firewall is not going to work

PHYSICAL CONTROLS ARE GOOD, BUT ...

Physical controls works but all you need is one employee to click on the wrong link and its game over !

SEPARATE WORK EMAIL FROM PERSONAL EMAIL

Business: TheRealPedro@gmail.com
Subscriptions: VoteforPedro@gmail.com
Junk: PedroJunkMail@gmail.com

EMAIL SECURITY

Are your emails private
Email attachments scanned
TLS enabled

PROTECTION

Why you should you protect your work email
It is part of my Work login , ADP, Paychex, Benefit Portal, 401K account login

FIREWALL

My employee clicked on the wrong link!

WHY SECURITY AWARENESS

THE HUMAN ELEMENT

This is the hardest part of security - we do not take time to teach our employees good cyber behavior. Traditionally this is done via fear factor.

NOT AN OPTION ANYMORE.

Your employees will behave the same way they do at home.

GREAT NEWS!

This has been proven - Recognition and awareness are key, this is why you must expose your employees to identify what a bad email or suspicious link look like.

IN THE OFFICE

Emphasis on what's relevant – Follow the money!
Think ... How can criminals get into my finances

SOCIAL MEDIA IS NOW ACCEPTED BEHAVIOR

Web, Email, Facebook, 24/7 – 365
You are being bombarded with data all day

HUMANS

WE ARE ALL DIFERENT

WE EMPHASIZED ON CHANGING BEHAVIOR

ONE PAGE, NO ATTACHMENTS

A picture is worth a 1000 words

We look at ways to make you want to change – This required your engagement

This was not another mandatory meeting, I needed to get to the place where you wanted to be there – I made the training personal !

FULLY ENGAGED

THIS WAS HARD

FIVE EMAIL DO'S AND DON'TS

Email has become one of the primary ways we communicate in our personal and professional lives. However, we can often be our own worst enemy when using it. In this newsletter, we will explain the most common mistakes people make and how you can avoid them in your day-to-day lives.

PRIVACY

Anyone who gains access to your email can read your messages. In addition, unlike a phone call or personal conversation, you no longer have control over an email once you send it. Your email can easily be forwarded to others, posted on public forums and may remain accessible on the internet forever. If you have something truly private to communicate, pick up the phone. It is also important to remember that email can be used as legal evidence in many countries. Finally, if you are using your work computer for sending email, keep in mind that your employer may have the right to monitor and read your email. If you use your work computer to access your personal email account, this could include your personal email. Check with your supervisor if you have questions about email privacy at work.

BCC/CC

WHAT IS IT?

"CC" stands for "carbon copy," which means you want to keep people copied and informed.

"BCC" means "blind carbon copy." It is similar to Cc, but no one can see the people you have BCC'ed.

THE PROBLEM

When someone sends you an email and has CC'ed people on it, you have to decide if you want to reply to just the sender or reply to everyone that was included on the CC.

When sending a sensitive email, you may want to copy someone privately using BCC, such as your boss. However, if your boss responds using "Reply All," all of the recipients will know that your boss was secretly BCC'd on your original email.

DISTRIBUTION LISTS

WHAT IS IT?

Distribution lists are a collection of email addresses represented by a single email address, sometimes called a mail list or a group name.

THE PROBLEM

Be very careful what you send to a distribution list, since so many people may receive that message. In addition, be very careful when replying to someone's email on a distribution list. You may only intend to reply to the individual sender, but if you hit "Reply All," you will have included the entire distribution list.

EMOTION

An email written in an emotional state could cause you harm in the future, perhaps even costing you a friendship or a job. Instead, take a moment and calmly organize your thoughts. If you have to vent your frustration, open Outlook, make sure it is not addressed to anyone and type exactly what you feel like saying. When you are done, get up and walk away from your computer, perhaps make yourself a cup of tea. When you come back, delete the email and start over again. Even better, pick up the phone and talk to the person, as it can be difficult to determine tone and intent with just an email.

AUTOCOMPLETE

WHAT IS IT?

As you type the name of the person you want to email, Outlook automatically selects their email address for you. This way, you do not have to remember the email addresses of all your contacts, just the recipient's name.

THE PROBLEM

The problem with autocomplete comes when you have contacts that share similar names. It is very easy for autocomplete to select the wrong email address for you.

EXAMPLE

you may intend to send an email with all of your organization's financial info to "Fred Smith," in accounting. Instead, autocomplete selects "Fred Johnson," your neighbor. As a result, you end up sending sensitive information to unauthorized people. To protect yourself against this, always double check the name and the email address before you hit send.

2FA

TWO-FACTOR AUTHENTICATION

I want to make you aware of a way to add an additional layer of protection beyond your password (called 2 factor authentication) to many of the accounts that you may currently have. It adds (in most cases) the ability to add a text message code sent to your phone before you can access accounts like the following: *Amazon, Fidelity Investments, Apple iTunes, Snapchat, Yahoo, Outlook, Google Mail, Apple, Twitter, Facebook, Dropbox, Google Drive, Chase, Bank of America, USAA, Wells Fargo, Skype, Vanguard, PayPal, and LinkedIn among others.*

Rey used 2FA to protect his accounts and is glad to see it at work. "The two-factor authentication works! It let me know when any of my accounts are accessed. In this case it wasn't a hacker with my credentials; my kids were using my computer and opened up the Google Chrome browser. My Gmail account automatically logged me in when they opened the browser and I received a text message notification of the login."

Suzanne used 2FA to protect her financial future. "It's scary to think that all my years of planning could be destroyed simply because someone stole my password."

2FA is a free security feature that prevents hackers from accessing your accounts, ***even if they know your password.***

LEARN HOW TO TURN ON 2FA FOR THE SITES AND APPS YOU USE *BY CLICKING THE LINK BELOW.*

CIMAREX

CEO FRAUD (frôd)

n. A deception practiced in which a cyber criminal will pretend to be a CEO or other senior executive in order to induce employees to give up information, perform wire transfers, give tax information, etc.

HOW DO CYBER CRIMINALS ATTEMPT CEO FRAUD ATTACKS?

Step 1.

Become a Cimarex Guru

Criminals search your company's website for information, such as where it is located, who your executives are, and other organizations you work with.

Step 2.

Research Employees

The criminals then learn everything they can about your coworkers on sites like LinkedIn, Facebook, or Twitter. Once they know your organization's structure, they begin to research and target specific employees. They pick their targets based on their specific goals. If the cyber criminals are looking for money, they may target staff in the accounts payable department. If they are looking for tax information, they may target human resources.

Step 3.

Craft the Attack

Once they determine what they want and whom they will target, they begin crafting their attack. Most often, they use spear phishing. Spear phishing is similar to phishing; however, instead of sending a generic email to millions of people, they send a custom email targeting a very small, select number of people. These emails are extremely realistic looking and hard to detect due to the detailed research the criminals have done.

Wire Transfer:
Who handles the organization's finances? *The criminals seek out their target employee and send an email pretending to be the target's boss. The email likely tells them there is an emergency and money has to be transferred right away to a certain account.*

Tax Fraud:
Who handles employee information? *The criminals could email someone in HR pretending to be a senior executive or someone from legal, demanding certain documents be provided immediately.*

Attorney Impersonation:
Not all CEO Fraud attacks involve just email; other methods, like the telephone, can be used. In this scenario, criminals start by emailing you pretending to be a senior leader, advising you that an attorney will call you about an urgent matter. They then call you pretending to be the attorney. The criminal creates a tremendous sense of urgency as they talk about time-sensitive, confidential matters.

HOW CAN YOU PROTECT YOURSELF AND YOUR ORGANIZATION?

Common sense is your best defense.

If you receive a message from your boss or a colleague and it does not sound or feel right, it may be an attack.

Clues can include:

- *Tremendous sense of urgency*
- *Signature that does not seem right*
- *Unexpected email tone*
- *Different name used than what the person actually calls you*

The attacker may even use an email address or phone number that you have never seen before, or an email address that is similar to your coworker's or boss's email. When in doubt, call the person at a trusted phone number or meet them in person (don't reply via email) and confirm if they sent the email. Never bypass security policies or procedures. Your organization may have policies that define proper procedures for authorizing the transfer of funds or the release of confidential information. A request that attempts to bypass these policies, regardless of their apparent source, should be considered suspicious and be verified before any action is taken.

SCAM-A-CLAUSE IS COMING TO TOWN.

Remember to watch out for the following holiday scams this season

REMEMBER TO USE 2FA

Many of the world's largest online and mobile properties offer 2FA (two factor authentication) to help prevent fraudulent activity and protect your accounts. To see if the sites and apps you use offer 2FA, and to get detailed step-by-step instructions on how to use it, click the link below.

MADE IT EASY TO REPORT SUSPICIOUS EMAIL

EMAIL

Create a unique email address to report suspicious emails. Take advantage of email systems that allows you to create email addresses with prebuilt filters

MAKE IT SO EASY THAT YOUR CEO WANTS TO USE IT

Implement a link in outlook for a “One Click” submission

- It has to be that easy or I am not going to use it.
- Educate you users on ways to report bad emails
- Send a newsletter advertising this new way to tell us

NO POINTING FINGERS

You must earn your employees trust
They must understand that you really want to help them

EASY
Submissions

BRIBE WITH FOOD

CREATE LUNCH AND LEARNS

The honey effect – you must provide free food
Some came because of the free food ... But they came, now I got their attention

NO MANDATORY MEETINGS

You wanted them to come because it was interesting – I started talking about Facebook, Email, Online presence, and how to freeze your credit

Convince upper management to give you $500

This was the hardest step - actually our first meeting was a pilot (test) ... It was so successful that after the first meeting we had a commitment to continue
The executive team understood the dynamic and importance of cyber education.

Food

The honey effect

CREATE COMPETITIONS

CONGRATULATE THE GROUPS THAT PASSED THE TEST

Let me tell you – Engineers like to win! - they created a spreadsheet that was posted in their offices to see who had clicked on the fake email

CREATED BUZZ ABOUT “PEDRO’S TRICKED EMAILS”

Many folks were intrigued as of why they had failed –This opened the door to education and deeper understanding in the ways that you can be tricked in an email.

GAMIFICATION

WE LEARN BEST WHEN HAVING FUN

MADE TRAINING FUN, ANIMATED, EASY GOING

IT WAS FUN – NOT I FAILED !

- This created acceptance, This was not the security guys trying to get me !
- Trust, I actually received calls of employees telling me that they had failed and that they would have never look at the “from” in the email … because everything else look legit.
- Elevator talks, I got daily questions on web, emails, or out of office etiquette

FUN TRAINING

EASY GOING

WHAT WE HAVE LEARNED

ITS HARD IT ABOUT PEOPLE BUT ITS POSSIBLE

- Email is the delivery method – lets learn how to stop it
- Technical controls work, but people are going to be people
- Security awareness – single most effective control for the least amount of money
- Behavior modification – Is key, so relate to what matters to your users - Home
- Make it easy to report bad emails
- Bribe with food ... The honey effect
- Make security awareness fun – acceptance factor
- Above all create trust and acceptance, YOU are not the enemy

You are an influencer

Use Every Opportunity

Lots of information – My goal is to make you aware of the power that you have… You are our best weapon against hackers! Ask questions. See something suspicious, reach out & let your security team know.

Pedro Serrano, CISSP
@InfoSecPedro

Family fun night ideas (The Challenge – Let have some fun and find the fake email)

- Phishing training … https://phishingquiz.withgoogle.com/
- Cybersecurity kids activity kit - https://www.knowbe4.com/cybersecurity-activity-kit

- https://www.campaignmonitor.com/blog/email-marketing/2018/03/shocking-truth-about-how-many-emails-sent/
- https://expandedramblings.com/index.php/email-statistics/
- US Email Statistics Report, 2016-2020 http://www.radicati.com
- https://blog.barkly.com/phishing-statistics-2016
- https://www.wombatsecurity.com/press-releases/new-report-state-of-phishing-attacks