SECURITY TRAINING

By Wyoming volunteers for non-technical Wyoming citizens

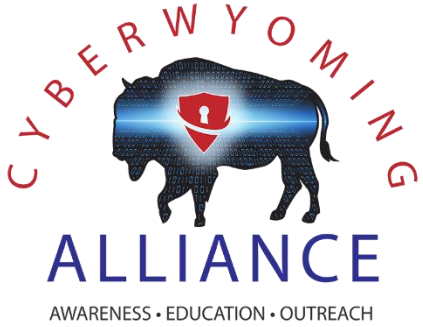
WYOCAN

WYOMING CYBERSECURITY ACTION NETWORK

Developed by Wyoming CAN Members

Neil McSweeney, Chief Information Officer at
Meridian Trust Federal Credit Union

In collaboration with Laura Baker,
President of the CyberWyoming Alliance

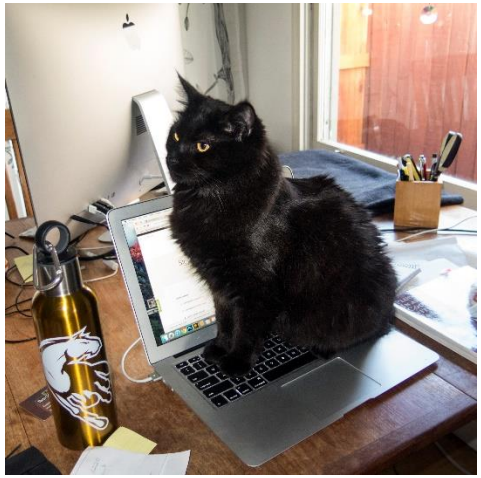


Brought to you by the volunteer run Wyoming CAN Committee members

Security VS Safety

Security: We must protect our computers and data in the same way that we secure the doors to our homes.

Safety: We must behave in ways that protect us against risks and threats that come with technology.



And sometimes the threats are from unexpected sources.

Security at Home

KNOWLEDGE is power!

- Secure your computer(s)
  https://youtu.be/DaDF5VDVDuI
- Secure your wi-fi
  https://youtu.be/t_BWIBBH1tU
  https://youtu.be/HcpNq8MRDzI
- Remember physical security
- Talk to your family or roommates about safety and security

Type of Attacks

- Adversaries (hackers, criminals) will attempt to take advantage of the people through
- Social Engineering
- Phishing
- Spyware
- Worm
- Virus
- Password
- Rootkits
- Botnets / Zombies
- Trojan/Logic Bomb
- Ransomware
- Man in the middle
- Evil Twin
- Buffer Overflow
- Credential stuffing

Social Engineering Within Emails

Messages that use humans curious nature, half stories.

Email contains a link that you just have to check out as you are curious.

- Your computer is now infected with malware, Hackers have control!
- **Email contain a download**–pictures, music, movie, document, etc.
- Download contains malicious software, Hackers have control!

Photo by mohamed hassan from PxHere

Social Engineering Within Emails

These emails may play on your heart string with a feel sorry situation or you won something

- **Email urgently ask for your help**

  Someone is stuck in a foreign country robbed, beaten or in hospital.

  They need you to send money.

  They tell you how to send the money to the criminal.

Warning Signs: Payment requests via wire transfer or gift cards!

Social Engineering Within Emails

Email claims to be from a lottery, or an unknown inheritance, or the millionth person to click on their site.

Need to provide your information (address , phone number, Social Security number, bank account) These are phishes that if fallen for by giving away their information bank account are emptied, and identity stolen.

Social Engineering Within Emails

Asks you to donate to their charitable fundraiser, or some other cause.

Includes instructions on how to send the money to the criminal.

Social Engineering Within Emails

The message may explain there is a problem

- You are required you to "verify" information by clicking on the displayed link.
- The link location may look legitimate with all the right logos and content.
- Complete a form providing information.
- Often these types of phishing scams include a warning of what will happen if you fail to act.

Criminals know that if they can get you to act before you think, you're more likely to fall for their phish.

Phishing

Phishing is a criminal mechanism employing both social engineering and technical subterfuge to steal users' personal identity data and financial account credentials.

Typically, a phisher sends an e-mail, IM (instant message), comment, or text message that appears to come from a legitimate, popular company, bank, school, or institution.

Normally involve a scenario or half-story.

Types of Phishing Attacks

Whaling

Targeting high level executives

Watering Hole Phishing

Infection a web site so devices downloads malware

Spear Phishing

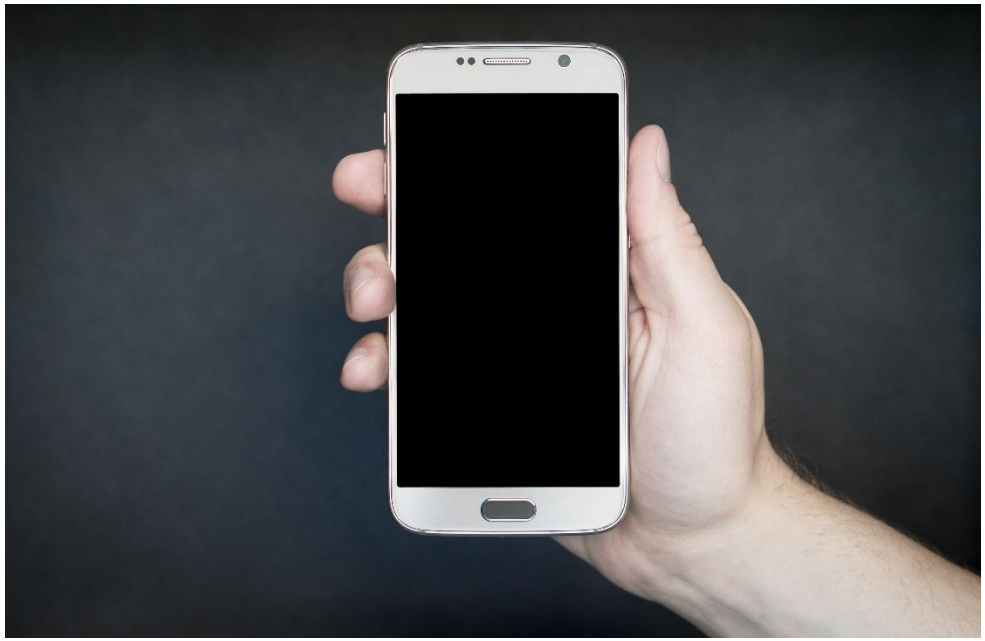
Targeting a certain individual

CEO Fraud

Send email from CEO to transfer funds

Types of Phishing Attacks

- Vishing …..Voice call asked to provide information (IRS, bank).



- Smishing ……Text messages lure users to download malicious programs.

Types of Phishing Attacks

Clone phishing

Creates a replica of legitimate message and sends from legitimate email address. Updated message contains malicious content.

Domain Spoofing

Email or fraudulent web site.

May change out the 1 or a I or an 0 or a O.

Phishing Attack – Obvious Example

From: Bank of Africa<AU> [mailto:Www.@pastel.ocn.ne.jp]
Sent: Tuesday, May 17, 2016 10:03 AM
Subject: Attention Dear Customer

The Director Of Operations Foreign Remittance Division, BOA Bank, Republic Du Benin, RB, Gordomew, Alakija Branch.

Attention Dear customer

This is David Mokwes, How do you want to receive your winning funds worth total sum of $Two million dollars? Choose one out of this two below options and get back to us urgent, The UN/IMF left with us a Check worth Two Million USD with instructions that you will contact us for it, We didn't hear from you for long then we decided to send our previous email to confirm if you are around or not, Just as i told them, it is a bit hard to mail a check from here. So I suggested to them that it would have been better/easier to get the cheque remitted for your Online Banking transfer or wire bank transfer, Therefore If the cheque is to be remitted like i told them, we will only need International Remittance Permit Certificate in-which will cost the sum of $150 for securing it hence other works are Okay. But this amount puts your funds into your account instantly. In other hand, if what you want us to convert the check into ATM visa Card and send to your address, then first there must be a VAT & stamp duty weather by ordinary mail or delivery company, this VAT/Stamp duty of your Card envelope will guide it till it gets to your door-step without any hitch or hassle, and all it will only cost is $90. In addition to that, your $Two million winning funds is a legal winning money doesn't have any illegal treat attach to it, therefore it is left for you to decide on what you want us to do then hurry and send the fee and email us the pick up confirmation info for procedure.

Your are advise to make haste in indicating one of these options once more and get the cost sent to us through Money Gram or Western Union at below information:

(1) Receiver's Name:=== Victor Obi
(2) Country:=== Benin republic OXF
(3) City:=== Cotonou
(4) Question:=== W
(5) Answer:=== T
(6) MTCN:===?

Note: I wish to inform you that we are real bank and can never ask for fees after fees, it is unprofessional to ask for unforeseen fees, Therefore we have verified things and calculated all due but find out that the only fee involve is as above listed at each option, so you have nothing to worry after the fee is paid OK!.

Go ahead choose one of these option and send the fee today immediately then you shall have your funds through your preferred means.

Kindly get back to us with your decision Urgent:

Thank you and have a great day ahead.

Yours Sincerely:
Mr. David Mokwes.
Bank of Africa AU Benin.

Phishing attack – a little less obvious

MedicarePlan.com

Affordable Medicare Supplement Plans Available Now!

Get A Personalized Plan From The Best Carriers!

We Help Get Access to **All Plans** at the **Best Rates**

Get My FREE Quote!

- Competitive Rates
- Compare Quotes in Real-Time
- Plans That Fit Any Budget

Learn more here

If you wish to unsubscribe from future mailings please click here or write to:
113 Cherry Street #88030, Seattle, WA 98104-2205

Congratulations!

Redacted Name - CLICK HERE

amazon

If you wish to unsubscribe click here
Or you may write to Space Tree Technologies at P.O. Box 4213,Nevada,US

Unsubscribe | Report Spam

Bath&ShowerPros

Remodel Your Bathroom and Save Big

Competitive Offers = Better Prices

Compare Estimates

Bath&ShowerPros.com can help you compare personalized offers from trusted remodelers in your area.

Whether you need a basic bathtub update, bathtub-to-shower conversion, or full bathroom remodel, we can help you find the right professionals at the right price.

Learn More

Phishing attack - a little less obvious

From: AppleID <no_rep@flax.com>
Date: April 18, 2017 at 11:07:28 AM MDT
To: Undisclosed recipients: ;
Subject: Account locked

Apple Store

Sent on Apr 18, 2017

Your account has been locked for security reasons.

We will hold your account for one week from the date of this email.

After that date, if your account informations aren't updated, your Account will be terminated and you will not be able to use it.

To unlock your account, please sign in and follow instructions.

SIGN IN

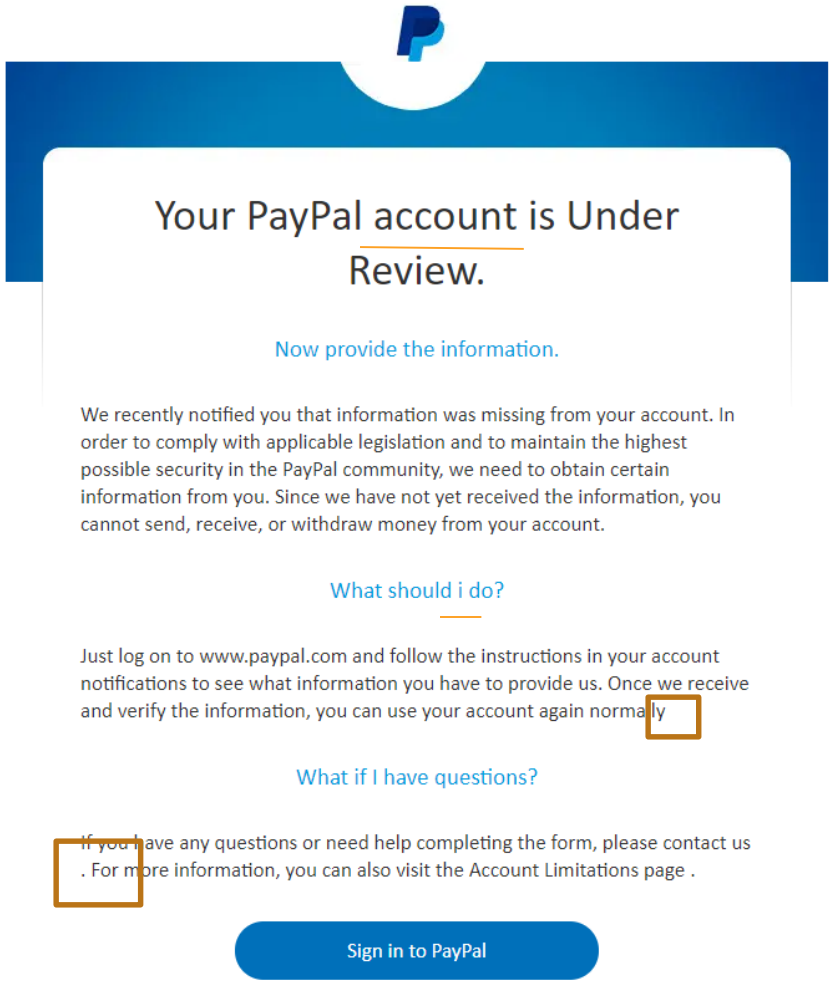
We are dedicated to protecting your information. Learn about our security measures and what we do to protect you online.

Please do not reply to this email.

Sincerely,

Phishing attack – a little less obvious

From: "service@intl.paypal.com" <buldsosades-ifs136s.c3wja62@keheednaaa.com>
Date: April 30, 2020 at 7:41:46 AM MDT
To: "customer@live.com" <customer@live.com>
Subject: Re: [Status Statement Added] New Information - Your account was restricted on : Thursday April 30, 2020.



Your PayPal account is Under Review.

Now provide the information.

We recently notified you that information was missing from your account. In order to comply with applicable legislation and to maintain the highest possible security in the PayPal community, we need to obtain certain information from you. Since we have not yet received the information, you cannot send, receive, or withdraw money from your account.

What should i do?

Just log on to www.paypal.com and follow the instructions in your account notifications to see what information you have to provide us. Once we receive and verify the information, you can use your account again normally

What if I have questions?

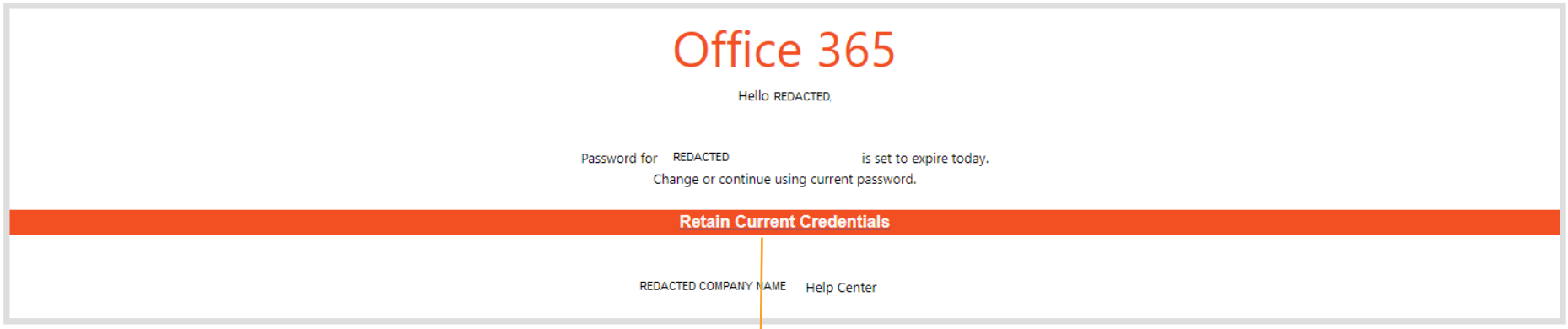
If you have any questions or need help completing the form, please contact us . For more information, you can also visit the Account Limitations page .

Sign in to PayPal

Phishing Attack – a little less obvious

easonj@seattleu.edu

From: MS/REDACTED CO NAME <easonj@seattleu.edu>
Sent: Thursday, February 25, 2021 7:49 AM
To: REDACTED
Subject: Password Notification for REDACTED at February 25, 2021, 2:48:54 PM



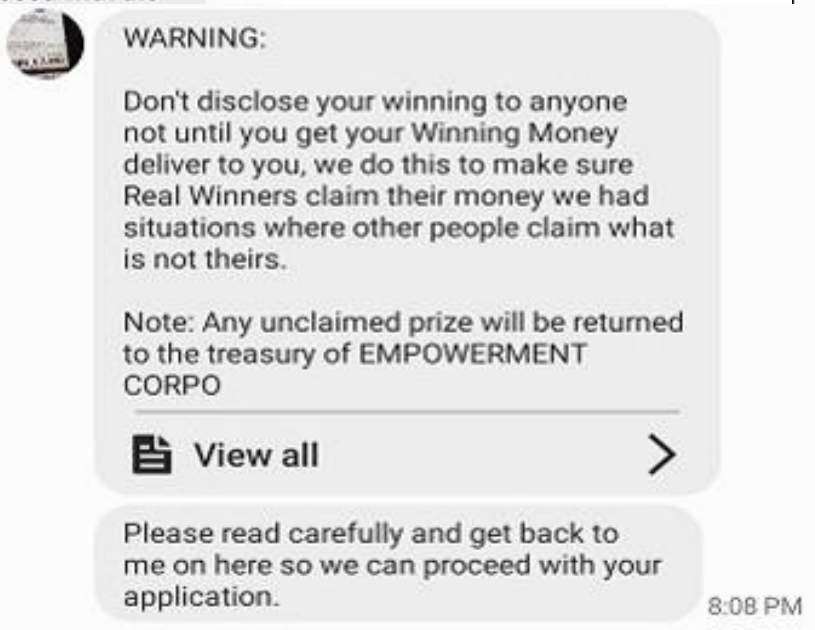
http://t.communication.lacapitale.com/r/?id=h8f65e76,10e690b9,11b4950e&p1=d-at.club/fr/consentement?refusForce=ZGNvbm5vcnNAdGF5bG9yY29uc3RydWN0aW9uLmJpeg==&scext=120-003-400-20-5102&telephone=18442816331

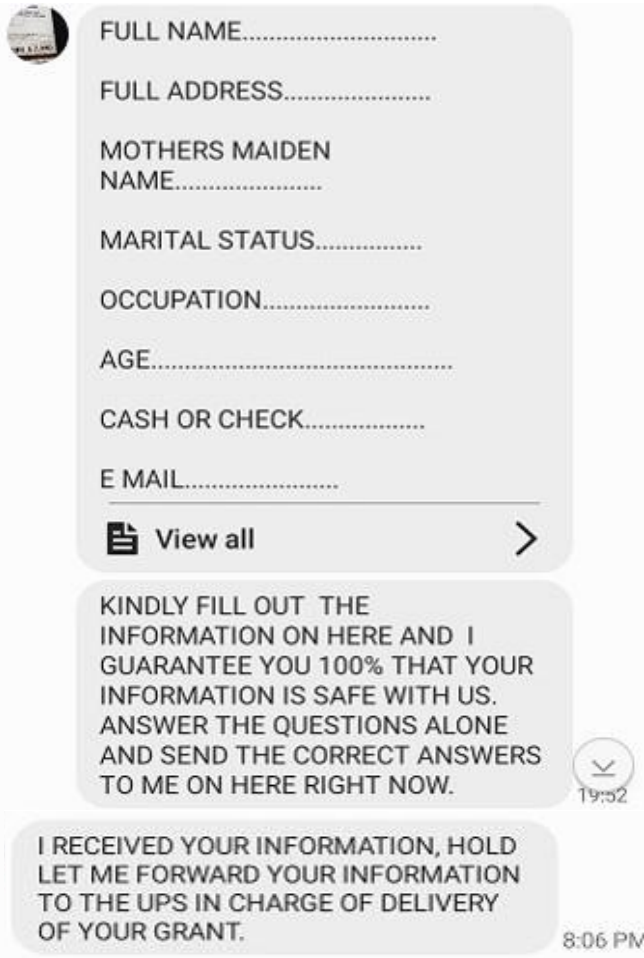
Social Media Phishing

Smishing

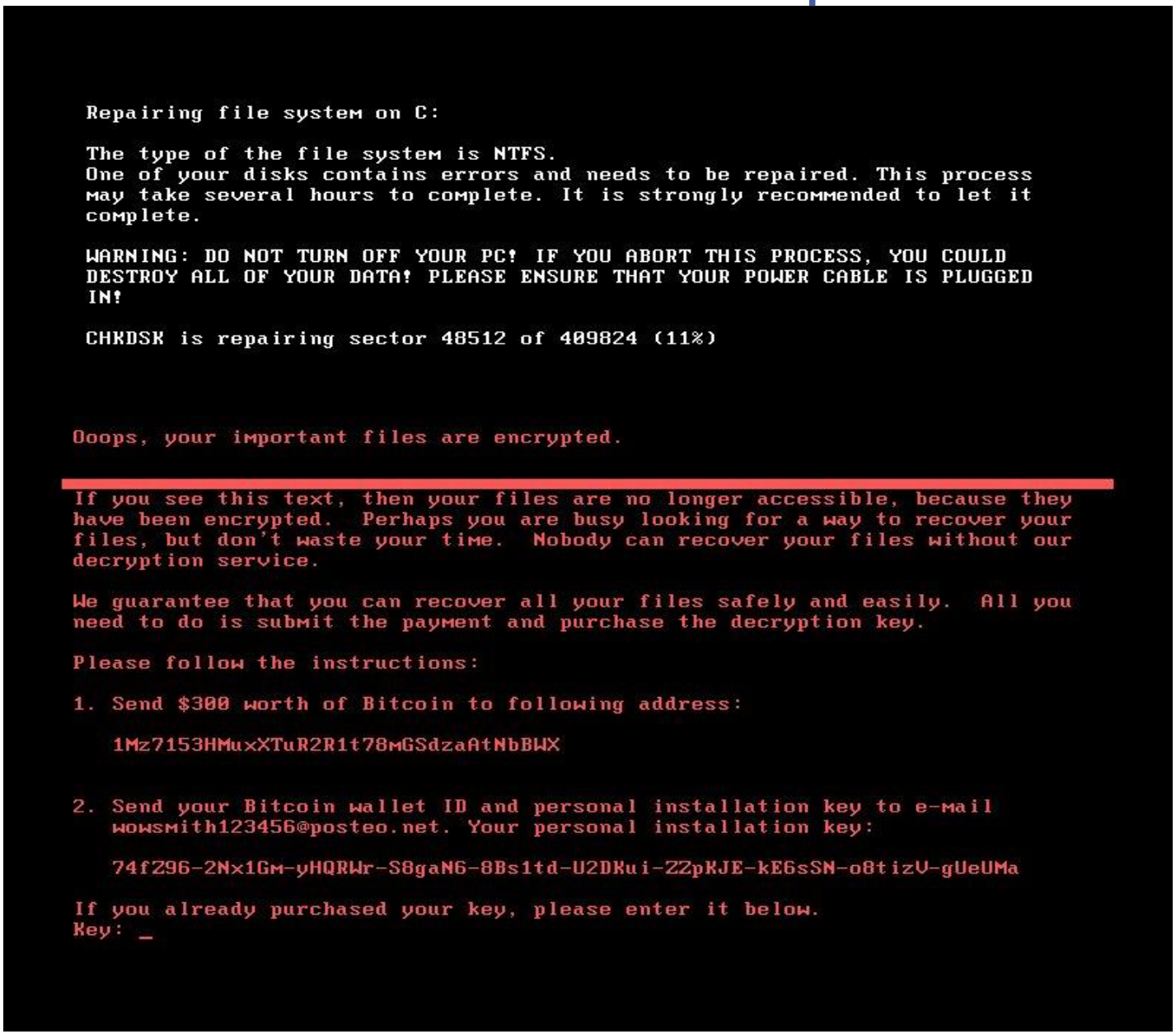
12:37
(321) 985-4935
3219854935
Friday, December 20, 2019
Hello madam Redacted , my name is Agent Thomas McCarthy from the board of Home Improvement Grant office. Redacted sent a text to me saying you want to apply for grant from our board. Get back to me now to proceed with the application.

Welcome this is to let you know that an on going federal gran organised by our board to help the society maintain good standard of living.
Thomas, my name is Redacted I live in ,Wy. My addres , I a widowed. I WOULD like a grant f home improvements!
19:46
Two billion dollars ($2,000,000,000 00) is placed on it and each beneficiary get $100,000. To apply, you have to fill the claim requirement form so that the UPS can locate you


WARNING:
Don't disclose your winning to anyone not until you get your Winning Money deliver to you, we do this to make sure Real Winners claim their money we had situations where other people claim what is not theirs.
Note: Any unclaimed prize will be returned to the treasury of EMPOWERMENT CORPO
View all
Please read carefully and get back to me on here so we can proceed with your application.
8:08 PM


FULL NAME.....
FULL ADDRESS.....
MOTHERS MAIDEN NAME.....
MARITAL STATUS.....
OCCUPATION.....
AGE.....
CASH OR CHECK.....
E MAIL.....
View all
KINDLY FILL OUT THE INFORMATION ON HERE AND I GUARANTEE YOU 100% THAT YOUR INFORMATION IS SAFE WITH US. ANSWER THE QUESTIONS ALONE AND SEND THE CORRECT ANSWERS TO ME ON HERE RIGHT NOW.
19:52
I RECEIVED YOUR INFORMATION, HOLD LET ME FORWARD YOUR INFORMATION TO THE UPS IN CHARGE OF DELIVERY OF YOUR GRANT.
8:06 PM

Ransomware - Plain and Simple – For Money!



HOW TO PROTECT YOURSELF

Hovering

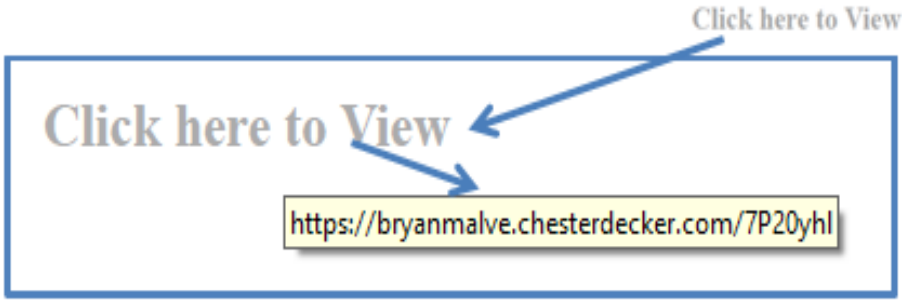
From: "Service Support" <HTGSP-1058456-HTGSP-1058456@HTGSP-1058456.dadhealth.chesterdecker.com>
To: [redacted]
Sent: Sun, Mar 15, 2020 at 17:28
Subject: Re: [Notice] receipt from your purchase 31041

Yahoo!

Two Factor Authentication.

Hello, [redacted] Your PayPal account has been disabled due to unusual transactions. Click below to cancel transaction(s). For added security to mitigate the latest trends in email data compromises,office Mail is rolling out compulsory Two-factor Authentication for it's email users.

Click here to View



Hovering over the link allows you to see where this is actually going. Note it isn't going to PayPal or Yahoo.

Hovering

From: OFFICE 365 <OFFICE-SUPPORT@office365.microsoft.com>
Sent: Monday, November 18, 2019 8:15 AM
To: updates1@office365.microsoft.com <updates1@office365.microsoft.com>
Subject: Re: VERIFICATION

--

OFFICE 365

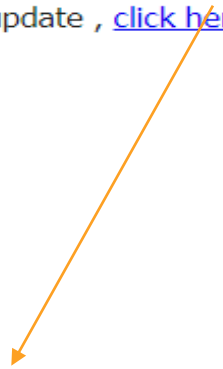
Your e-mail needs to be updated with our newly released 365-Secure Internet Security 2020 version of a better resource web-mail spam and viruses update.

Failure to update correctly will process your email account being temporarily blocked or suspended from our network

For verification and update , click here.

Thanks,

LocalHost



https://forms.gle/Munm1xrREnTPUm4L9

Hovering

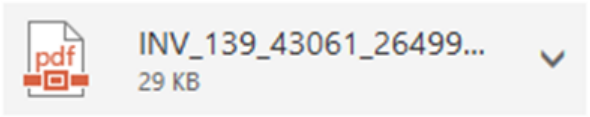
From:
Sent: Friday, July 12, 2019 1:20 PM
To:
Subject: Attached - 20463633_534r436538_

INV_139_43061_26499...
29 KB

See attached. Can you please confirm and preview

Thank you for your business – we appreciate it very much.

Thanks,



When you hover, it links you to a malicious site to change your credentials

https://disq.us/?url=https%3A%2F%2Fwaa.ai%2F3z7C&key=KdAMdeC2uPZRCMfoUJduvQ

Owner

It had the business's address & phone #

Password Security

- **Password :** The role of a password is to prevent unauthorized access to data just as a key prevents unauthorized access to a house or apartment.
  - **DO NOT** share passwords (even if they claim to be IT help!)
  - **DO NOT** keep passwords in plain sight at home.
  - Use complex password Combining words using symbols and numbers
    - Example: Southampton FC = S0uth@mpTH0n F(
    - Abbreviating a phrase or use music lyrics, poems or quotes

LIE about your password reset questions

https://youtu.be/jcLiVrderE4

Password Recommendations

- Don’t reuse passwords across sites https://youtu.be/zIriU1NL4v0
- A good password is:
  - **Private**: it is used and known by one person only
  - **Secret**: it does not appear in clear text in any file or program or on a piece of paper pinned to the terminal
  - **Easily remembered**: so there is no need to write it down
  - **At least 12 characters, complex**: a mixture of at least 3 of the following: upper case letters, lower case letters, digits and punctuation
  - **Not guessable** by any program in a reasonable time, for instance less than one week.
  - **Changed regularly**: a good change policy is every 3 months
- Beware that someone may see you typing it. If you accidentally type your password instead of your login name, it may appear in system log files

Remember to change your home network passwords!

How You Can Help Protect

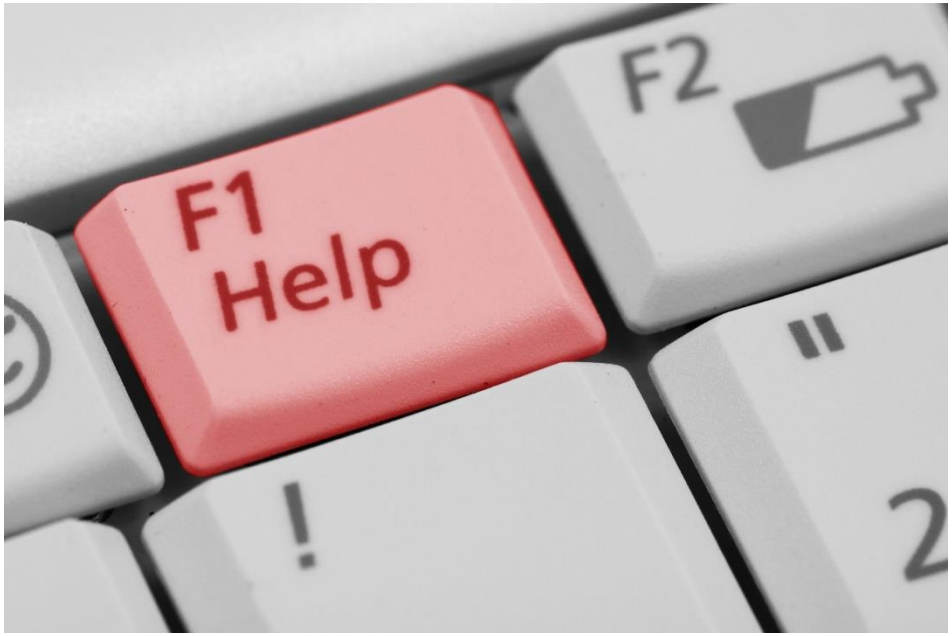
Best Practices for Home:

- Lock up information, and do not leave it lying around.
- Lock your computer when you are away.
- Grey out /truncate sensitive information when using it as an example.
- Lock file cabinet drawers that contain sensitive info.
- Don’t share your password.
- Ask questions, question stories, be skeptical.
- Get a home shredder.
- Do not open email attachments unless you are expecting the email with the attachment and you trust the sender.
- Do not click on links in emails unless you are absolutely sure of their validity.
- Only visit or download software from web pages you trust.

What to do if you click?

There's no shame….

If you click…even FBI cyber crimes agents have said they have clicked on something they shouldn't.



If it is user/password related – change your password right away.

Call your bank if you think there may be a compromise.

Notify friends, family & neighbors that 'this isn't you.'

Call an IT company to run a scan on your computer.

Call law enforcement if it is a large amount of money (FBI Internet Crimes Complaint Center https://www.ic3.gov/default.aspx)

Questions
Share Your Ideas With Us!
We are continuously improving

WYOCAN
WYOMING CYBERSECURITY ACTION NETWORK