PALITTO CONSULTING SERVICES

Wadsworth Chamber Cybersecurity

Introduction to Ben

- Wadsworth Resident
- Information Technology background from United States Marine Corps
- Bachelor's Degree in Cybersecurity from The University of Akron
- Current role at PCS in improving cybersecurity for SMBs

PCS
PALITTO CONSULTING SERVICES
25 YEARS OF SERVICE

Ransomware is the End Goal for Cybercriminals

- 20 Billion Dollar industry in 2021
- Persistent foothold is established in your network
- Ransomware is launched
- Encrypts all the data on your computers/servers
- Hold the decryption key ransom
- Just because you pay doesn't mean you get the decryption key
- Don't always need an expensive fancy box that sits on your network rack
- SMBs are targets

PCS
PALITTO CONSULTING SERVICES

5 Things Small Businesses Should Be Doing

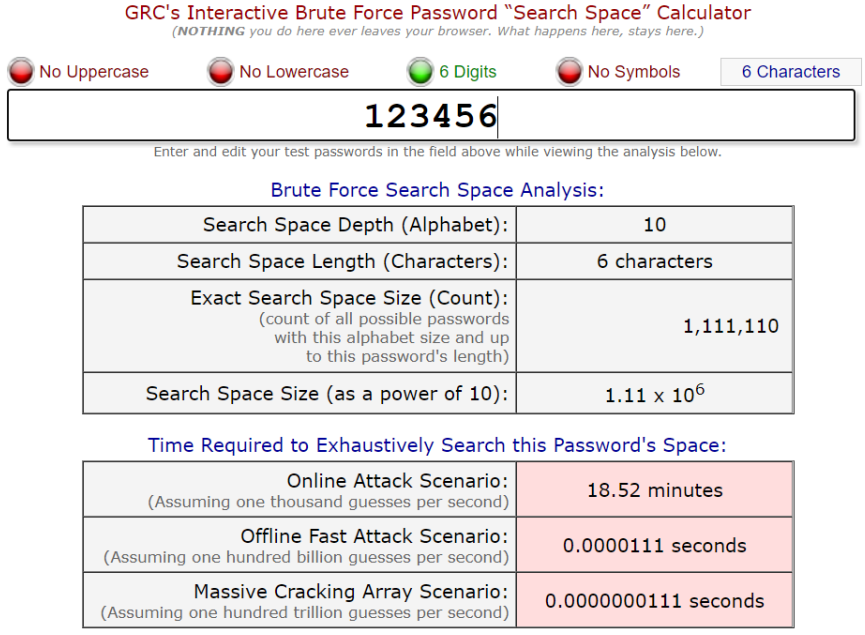
- **Passwords and 2FA**
  - Complexity requirements, how often they should be changed, and the criticality of two-factor authentication
- **Phishing Awareness**
  - The Human Firewall is the most important part of cybersecurity
- **Backups**
  - What is a backup and why they should be tested
- **Antivirus: Traditional or Next Gen**
  - Why free and “old school” antivirus doesn’t cut it anymore when it comes to ransomware
- **Vulnerability Management**
  - What on your network is exposed to the Internet and how that can leave you susceptible to attack

Passwords and 2FA

- Passwords that change often or passphrases that change less frequently?
  - 123456 versus How Now Brown Cow
- Danger of re-used passwords – data breaches
- Password Managers – cloud or local
- 2FA is very easy and free to implement - Combines something you **know** with something you **have**
- SMS vs Authenticator App
- Email and VPN are the two critical systems that must have 2FA
- Pipeline Attack – leaked credentials combined with VPN without 2FA

Passwords and 2FA Action Items

- GRC Haystack
- HaveIBeenPwned



GRC's Interactive Brute Force Password "Search Space" Calculator

*(**NOTHING** you do here ever leaves your browser. What happens here, stays here.)*

No Uppercase | No Lowercase | 6 Digits | No Symbols | 6 Characters

123456

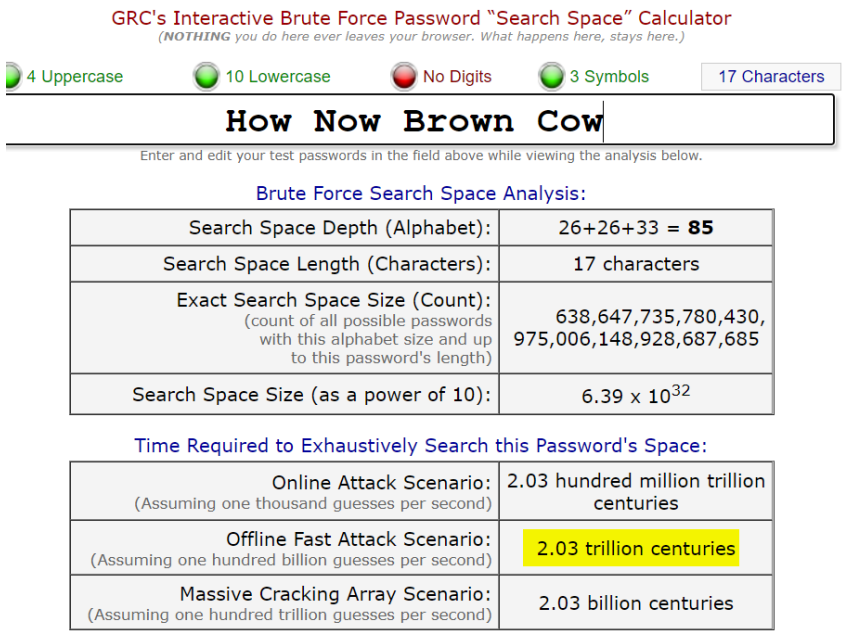
Enter and edit your test passwords in the field above while viewing the analysis below.

Brute Force Search Space Analysis:

Search Space Depth (Alphabet):	10
Search Space Length (Characters):	6 characters
Exact Search Space Size (Count): (count of all possible passwords with this alphabet size and up to this password's length)	1,111,110
Search Space Size (as a power of 10):	1.11×10^6

Time Required to Exhaustively Search this Password's Space:

Online Attack Scenario: (Assuming one thousand guesses per second)	18.52 minutes
Offline Fast Attack Scenario: (Assuming one hundred billion guesses per second)	0.0000111 seconds
Massive Cracking Array Scenario: (Assuming one hundred trillion guesses per second)	0.0000000111 seconds



GRC's Interactive Brute Force Password "Search Space" Calculator

*(**NOTHING** you do here ever leaves your browser. What happens here, stays here.)*

4 Uppercase | 10 Lowercase | No Digits | 3 Symbols | 17 Characters

How Now Brown Cow

Enter and edit your test passwords in the field above while viewing the analysis below.

Brute Force Search Space Analysis:

Search Space Depth (Alphabet):	26+26+33 = **85**
Search Space Length (Characters):	17 characters
Exact Search Space Size (Count): (count of all possible passwords with this alphabet size and up to this password's length)	638,647,735,780,430, 975,006,148,928,687,685
Search Space Size (as a power of 10):	6.39×10^{32}

Time Required to Exhaustively Search this Password's Space:

Online Attack Scenario: (Assuming one thousand guesses per second)	2.03 hundred million trillion centuries
Offline Fast Attack Scenario: (Assuming one hundred billion guesses per second)	2.03 trillion centuries
Massive Cracking Array Scenario: (Assuming one hundred trillion guesses per second)	2.03 billion centuries

Phishing Awareness

- Business Email Compromise (BEC)
  - **Number One** form of compromise
  - Accounting, HR, and Leadership are biggest targets
- Real Life Phishing Stories we see every day
- Phishing Campaigns Increase Employee Awareness
- Email 2FA and Employee Training is the best defense

Phishing Awareness Action Items

- Wizer-Training
  - Free security awareness training for individuals
- Hook Security
  - Fully automated phishing awareness training
- Sophos PhishThreat
  - Automated phishing awareness training or create your own

Car lights left on

HR

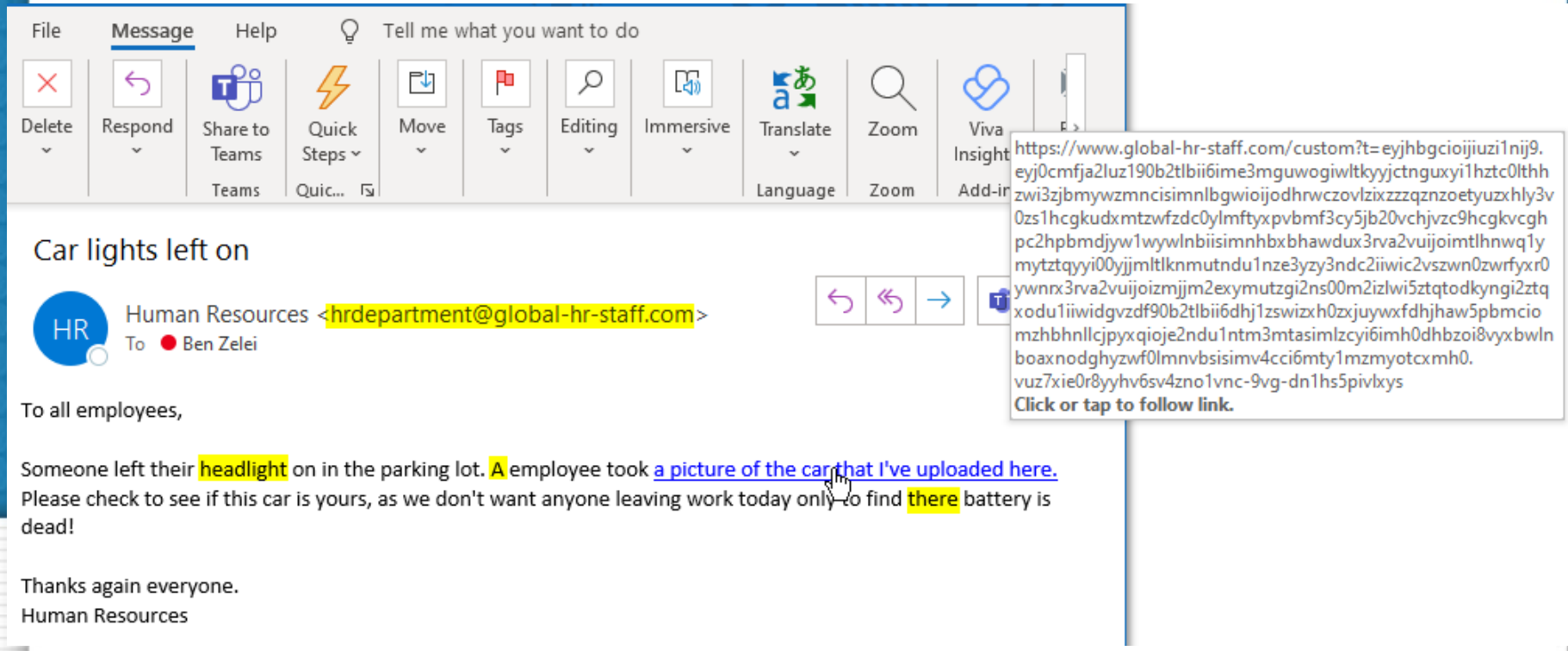
Human Resources <hrdepartment@global-hr-staff.com>
To Ben Zelei

13:15

To all employees,

Someone left their headlight on in the parking lot. A employee took a picture of the car that I've uploaded here. Please check to see if this car is yours, as we don't want anyone leaving work today only to find there battery is dead!

Thanks again everyone.
Human Resources


File
Message
Help
Tell me what you want to do
Delete
Respond
Share to Teams
Teams
Quick Steps
Quic...
Move
Tags
Editing
Immersive
Translate
Language
Zoom
Zoom
Viva Insights
Add-in
Car lights left on
HR
Human Resources <hrdepartment@global-hr-staff.com>
To Ben Zelei
https://www.global-hr-staff.com/custom?t=eyjhbgcioijiuzi1nij9.eyj0cmfja2luz190b2tlbii6ime3mguwogiwltkyyjctnguxyi1hztc0lthhzwi3zjbmywzmncisimnlbgwioijodhrwczovlzixzzzqznzoetyuzxhly3v0zs1hcgkudxmtzwfzdc0ylmftyxpvbmf3cy5jb20vchjvzc9hcgkvcghpc2hpbmdjyw1wywlnbiisimnhbxbhawdux3rva2vuijoimtlhnwq1ymytztqyyi00yjjmltlknmutndu1nze3yzy3ndc2iiwic2vszwn0zwrfyxr0ywnrx3rva2vuijoizmjjm2exymutzgi2ns00m2izlwi5ztqtodkyngi2tqxodu1iiwidgvzdf90b2tlbii6dhj1zswizxh0zxjuywxfdhjhaw5pbmciomzhbhnllcjpyxqioje2ndu1ntm3mtasimlzcyi6imh0dhbzoi8vyxbwlnboaxnodghyzwf0lmnvbsisimv4cci6mty1mzmyotcxmh0.vuz7xie0r8yyhv6sv4zno1vnc-9vg-dn1hs5pivlxys
Click or tap to follow link.
To all employees,
Someone left their headlight on in the parking lot. A employee took a picture of the car that I've uploaded here.
Please check to see if this car is yours, as we don't want anyone leaving work today only to find there battery is dead!
Thanks again everyone.
Human Resources

Backups

- What is *actually* being backing up?
  - Is that backup being tested?
- OneDrive/Google Drive/DropBox are not backups
  - They are file sync solutions
- File/Folder backup or Full System Image backup
- Onsite backup or Offsite backup
  - Backups are targets of ransomware
  - Immutable backups are critical
  - Built in Windows Backup - Onsite
  - Synology NAS - Onsite
  - N-Able Cloud Backup – Offsite/Cloud
  - Acronis Cloud Backup – Offsite/Cloud
  - Veeam Backup – Onsite/Offsite/Cloud

Antivirus: Traditional or Next Gen

- Traditional Antivirus
  - Generally only do signature scanning
  - Can't respond to a threat it's never seen before
  - Webroot, Malwarebytes, McAfee, Norton

- Next Gen Antivirus
  - Relies more on AI, machine learning, and process monitoring
  - Can respond to Zero Day Attacks
  - Sophos Intercept X, SentinelOne, CrowdStrike Falcon
    - Sophos Intercept X Home – home.sophos.com – 10 devices for $45/year

Vulnerability Management - Internal

- Ransomware if often launched on unpatched systems
  - Old Windows 7 computer (EoL Jan 2020)
  - Windows 10 computer that hasn't been updated in months
  - Windows Server Updates (Server 2012R2 going EoL Oct 2023)
  - Firewall/switch/server firmware out of date
- Have a patch plan system in place
  - Manually hitting check for updates on each Windows computer
  - Automated patching done through a system like an RMM (remote monitoring and management tool)
- Segment IoT devices into separate network
  - IoT devices (smart devices)
  - Cameras
  - Phones

Vulnerability Management - External

- Do you have any machines on your network exposed directly to the Internet?
  - Email server, FTP server, open RDP
  - Enable country blocking on firewall for these open systems
  - Segment these publicly available systems into a DMZ
  - Hafnium
- Internet Exposure Scans
  - grc.com/shieldsup
    - Very basic port scanning – can tell you what ports you have exposed
  - Vonahi Exposure Scout
    - vonahi.io/resources/internet-exposure-scan
    - More in-depth external scan, free but Vonahi will reach out to you
  - CISA Cyber Hygiene Vulnerability Scan
    - Free to federal, state, local, tribal, and territorial governments, as well as public and private sector critical infrastructure organizations
    - This does actual vulnerability scanning

Summary

- 2FA everything you can
- Train your users to spot phishing emails
- Take a second look at your backups
- Evaluate your antivirus solutions to determine if they can handle modern threats
- Update and Upgrade outdated systems – have a patch plan in place

Thank You!

Ben Zelei
benz@palittoconsulting.com

PCS
PALITTO CONSULTING SERVICES
25 YEARS OF SERVICE

Palitto Consulting Services
150 Main Street • Wadsworth, OH 44281
P: 330.335.7271
www.palittoconsulting.com