Cybersecurity 2022

Karl W. Palachuk
karlp@smallbizthoughts.com

Small Biz Thoughts

Copyright © 2021 Karl W. Palachuk – www.Smallbizthoughts.com

Agenda

- Cybersecurity basics – setting the stage
- Password security
- Email security
- Recommendations

Copyright © 2021 Karl W. Palachuk – www.Smallbizthoughts.com

Cybersecurity Basics

Copyright © 2021 Karl W. Palachuk – www.Smallbizthoughts.com

Recent Cybersecurity News

- *Ransomware* is actually down in the last two years
  - Ransomware: Malware that encrypts all the data it can find and demands a payment in order to receive the encryption keys

- But the cost per incident has more than doubled
  - 2019: Average cost to remediate = $761,000
  - 2020: Average cost to remediate = $1,850,000

- If you pay the ransom: About 65% of data is recovered

Copyright © 2021 Karl W. Palachuk – www.Smallbizthoughts.com

Recent Cybersecurity News

- Reported cybersecurity incidents are up 800% since the pandemic started
  - See FBI Internet Crime Complaint Center

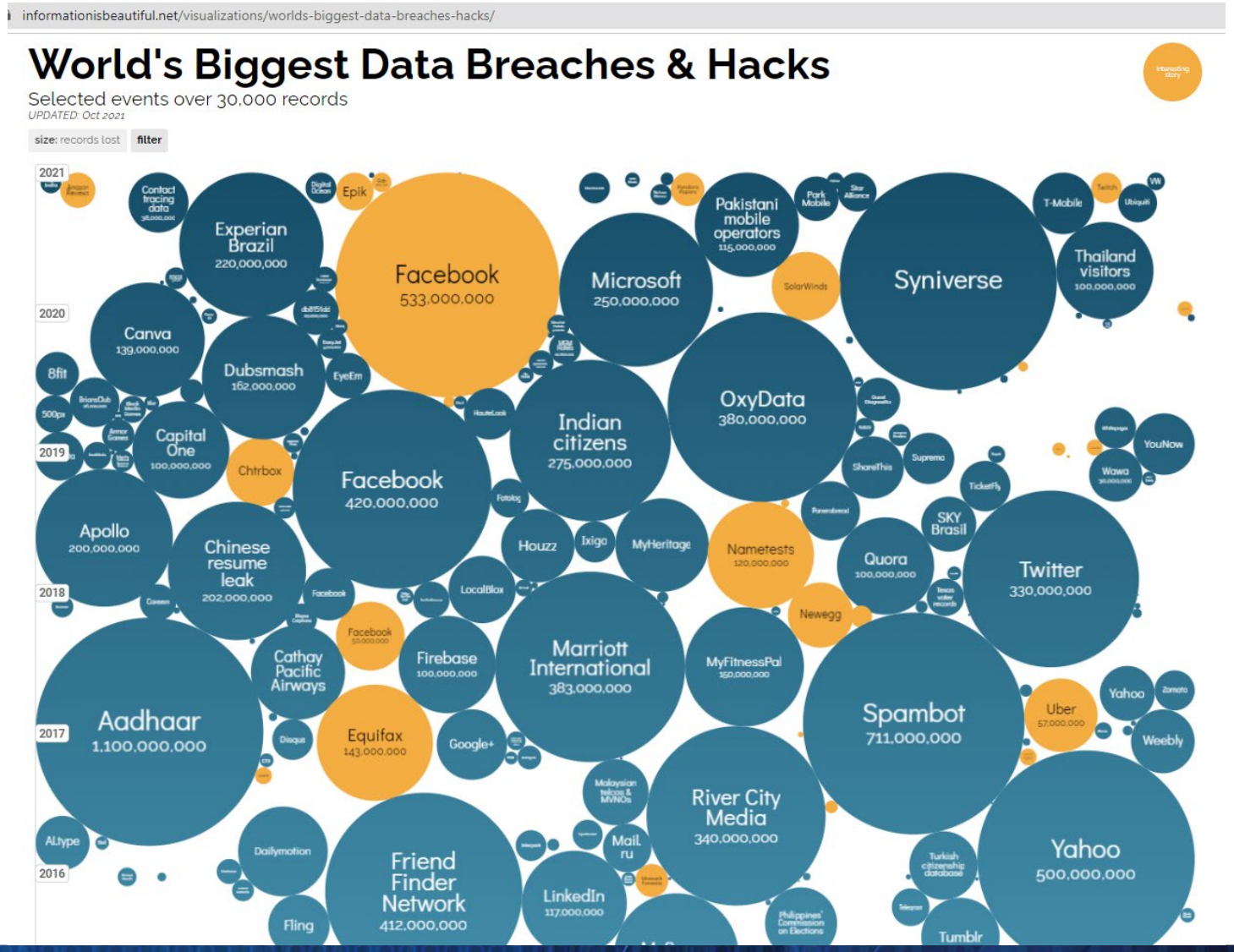
> "Cybercrime is now larger than all other forms of organized crime put together."
>
> – Michael George, Navigate

Copyright © 2021 Karl W. Palachuk – www.Smallbizthoughts.com

Largest Attacks

As the technology used in attacks gets better,

the number of large data breaches grows



https://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

Copyright © 2021 Karl W. Palachuk – www.Smallbizthoughts.com

What Are We Defending Against?

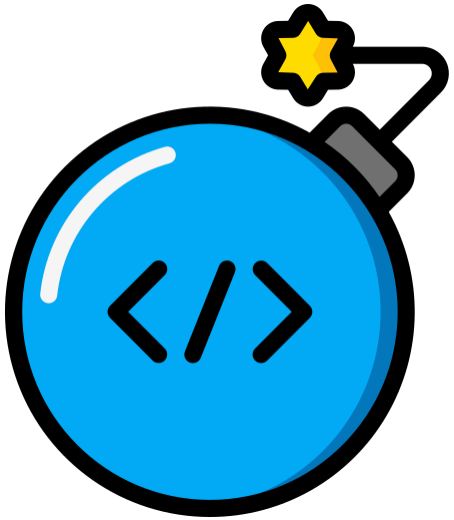
- Confidentiality
  - Unauthorized Access or Modification
- Integrity
  - Unchanged or un-deleted
- Availability
  - Ransomware or Denial of Service

Copyright © 2021 Karl W. Palachuk – www.Smallbizthoughts.com

There Is No "Targeting"

- Emails, passwords, web sites . . .
  - *Billions* of random attacks every day

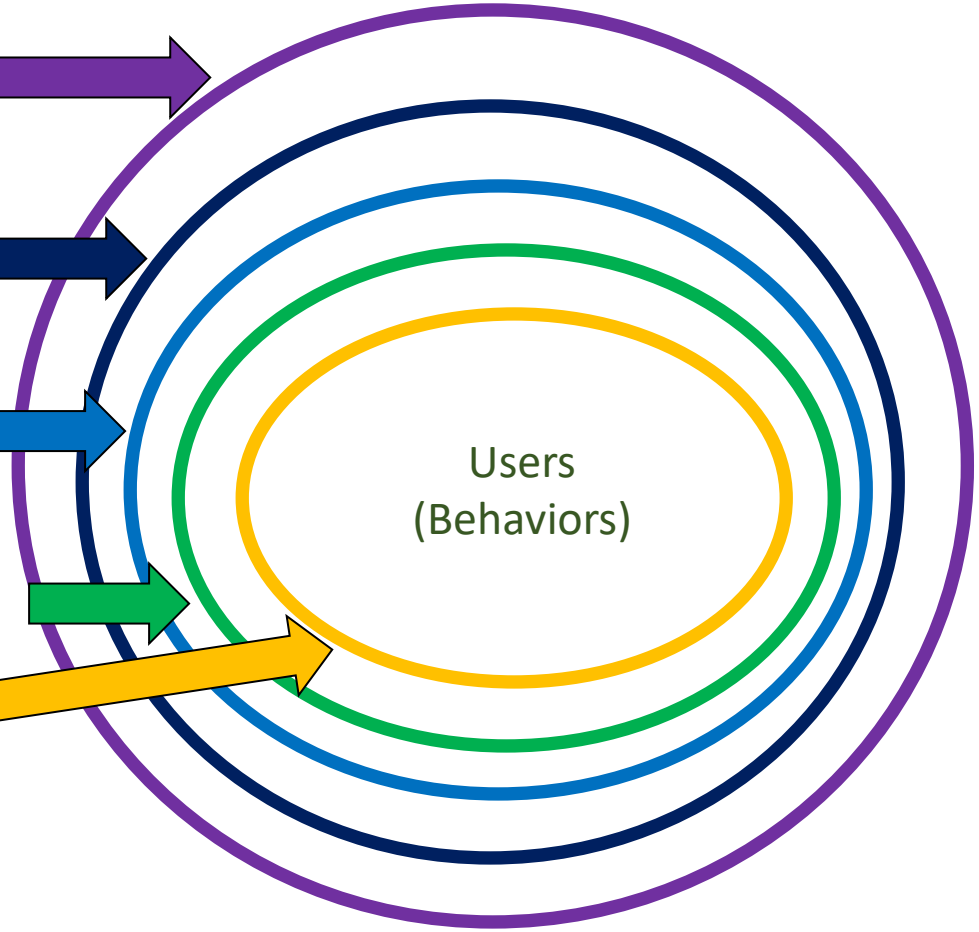
- Average days a system is breached before the breach is identified: **206** !
  - (IBM, 2019)



Copyright © 2021 Karl W. Palachuk – www.Smallbizthoughts.com

Attack Vectors: Everything!

- Firewall
- AV on Server
- AV on Desktop
- Patches, fixes, updates
- Policies



Copyright © 2021 Karl W. Palachuk – www.Smallbizthoughts.com

Password Security

Copyright © 2021 Karl W. Palachuk – www.Smallbizthoughts.com

The Basics: Passwords

- Use truly random passwords that no one could remember
  - e.g., V#i1Wt?68gM(!1PtB6)b
  - Use a password manager or vault
- Do not re-use passwords
- Give “fake” additional information
- Use 2-Factor Authentication

TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	1 sec	5 secs
7	Instantly	Instantly	25 secs	1 min	6 mins
8	Instantly	5 secs	22 mins	1 hour	8 hours
9	Instantly	2 mins	19 hours	3 days	3 weeks
10	Instantly	58 mins	1 month	7 months	5 years
11	2 secs	1 day	5 years	41 years	400 years
12	25 secs	3 weeks	300 years	2k years	34k years
13	4 mins	1 year	16k years	100k years	2m years
14	41 mins	51 years	800k years	9m years	200m years
15	6 hours	1k years	43m years	600m years	15 bn years
16	2 days	34k years	2bn years	37bn years	1tn years
17	4 weeks	800k years	100bn years	2tn years	93tn years
18	9 months	23m years	6tn years	100 tn years	7qd years

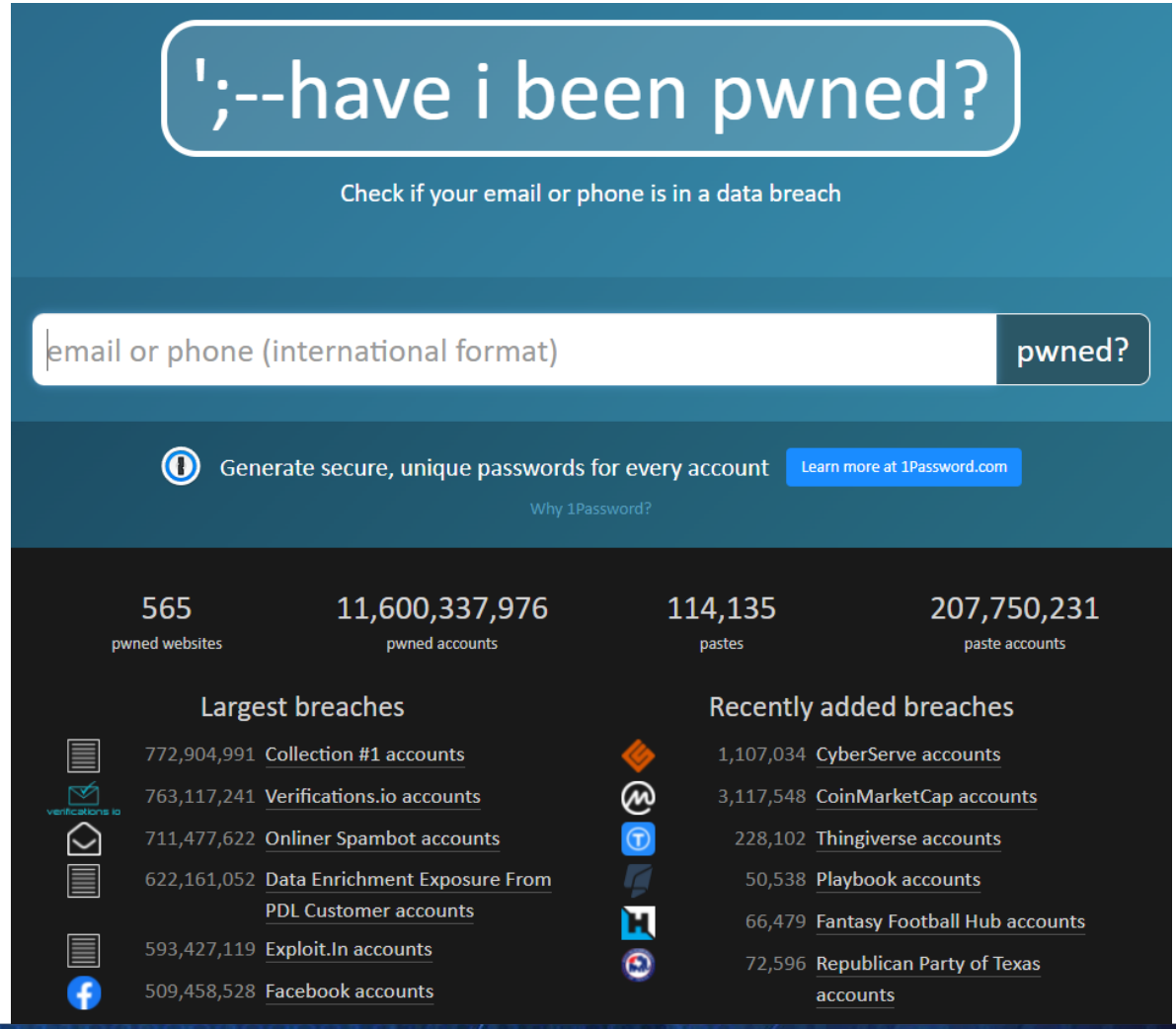
HIVE SYSTEMS

-Data sourced from HowSecureismyPassword.net

Copyright © 2021 Karl W. Palachuk – www.Smallbizthoughts.com

Your Password Has Been Compromised

- Almost certainly
- See https://haveibeenpwned.com
- As of last week . . .
  - 565 web sites
  - 11.6 billion accounts compromised



Copyright © 2021 Karl W. Palachuk – www.Smallbizthoughts.com

2FA / MFA

- Two-Factor or Multi-Factor Authentication

- Microsoft Authenticator
- Google Authenticator
- Email
- SMS ← Not as secure

Copyright © 2021 Karl W. Palachuk – www.Smallbizthoughts.com

Password Vaults or Managers

- LastPass
- Keeper
- Zoho Vault
- Dashlane
- Bitwarden
- 1Password
- LogMeOnce
- Password Boss
- Nordpass
- StickyPassword
- McAfee
- RoboForm

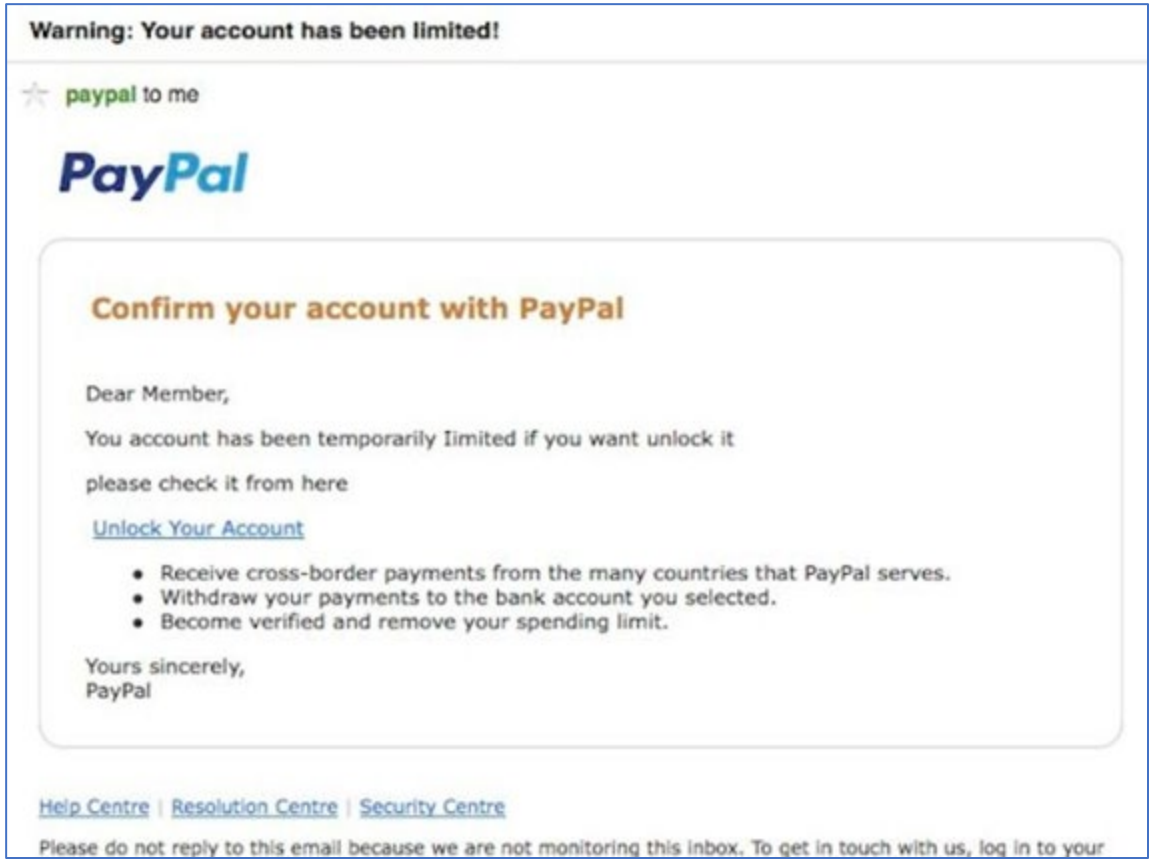
Copyright © 2021 Karl W. Palachuk – www.Smallbizthoughts.com

Email Security

Copyright © 2021 Karl W. Palachuk – www.Smallbizthoughts.com

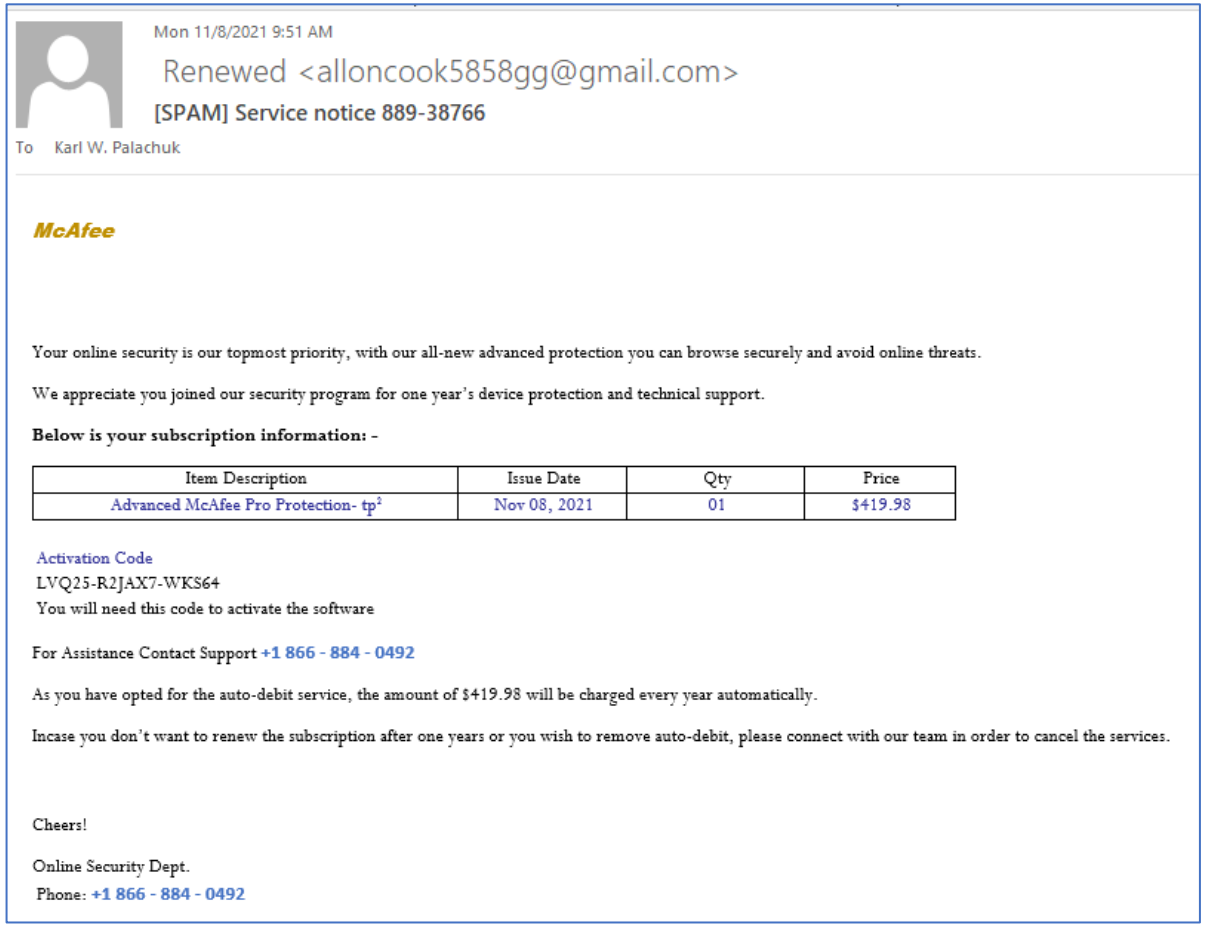
Emails and Social Engineering

- Their goal: Trick you into clicking!
  - Malware of some kind
  - Often ransomware
- . . . Or taking specific actions
  - Phishing
  - e.g., Wire money



Copyright © 2021 Karl W. Palachuk – www.Smallbizthoughts.com

You Received a Document (or Payment)!



Mon 11/8/2021 9:51 AM

Renewed <alloncook5858gg@gmail.com>

[SPAM] Service notice 889-38766

To Karl W. Palachuk

McAfee

Your online security is our topmost priority, with our all-new advanced protection you can browse securely and avoid online threats.

We appreciate you joined our security program for one year's device protection and technical support.

Below is your subscription information: -

Item Description	Issue Date	Qty	Price
Advanced McAfee Pro Protection- tp[2]	Nov 08, 2021	01	$419.98

Activation Code
LVQ25-R2JAX7-WKS64
You will need this code to activate the software

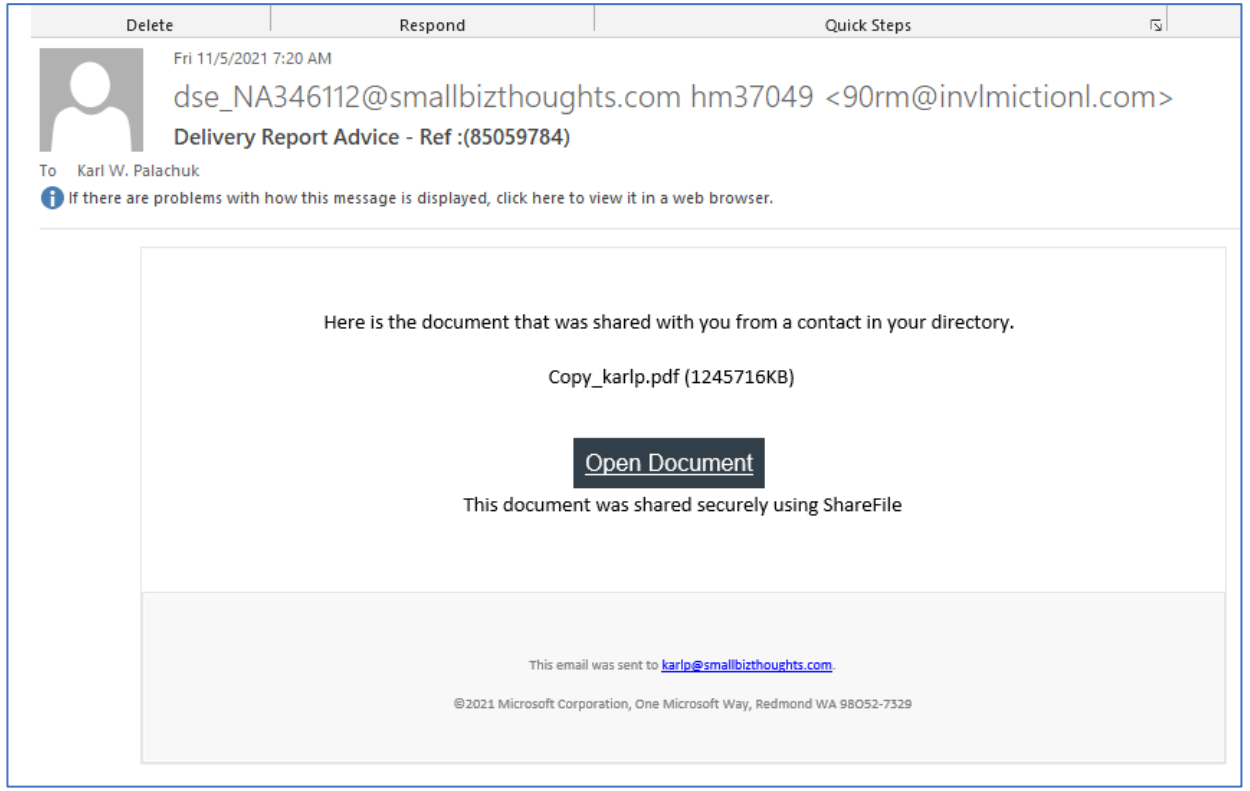
For Assistance Contact Support +1 866 - 884 - 0492

As you have opted for the auto-debit service, the amount of $419.98 will be charged every year automatically.

Incase you don't want to renew the subscription after one years or you wish to remove auto-debit, please connect with our team in order to cancel the services.

Cheers!

Online Security Dept.
Phone: +1 866 - 884 - 0492



Delete | Respond | Quick Steps

Fri 11/5/2021 7:20 AM

dse_NA346112@smallbizthoughts.com hm37049 <90rm@invlmictionl.com>

Delivery Report Advice - Ref :(85059784)

To Karl W. Palachuk

If there are problems with how this message is displayed, click here to view it in a web browser.

Here is the document that was shared with you from a contact in your directory.

Copy_karlp.pdf (1245716KB)

Open Document

This document was shared securely using ShareFile

This email was sent to karlp@smallbizthoughts.com.

©2021 Microsoft Corporation, One Microsoft Way, Redmond WA 98052-7329

Copyright © 2021 Karl W. Palachuk – www.Smallbizthoughts.com

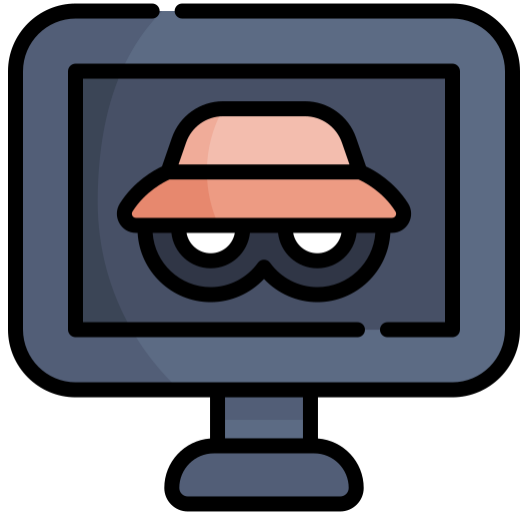
Email Security

- Banks, etc. will not send important information directly in email
  - Go to their site on your own
- Do not open email from people you don't know
- Do not open attachments unless you asked that person to send you that attachment
- When in doubt – DELETE!

Copyright © 2021 Karl W. Palachuk – www.Smallbizthoughts.com

Email and Web Safety

- Float Over Links . . .
- Shortened Links . . .
  - http://bit.ly/sample
- Hidden Extensions
  - SafeLookingFile.jpg
  - SafeLookingFile.jpg.exe



Copyright © 2021 Karl W. Palachuk – www.Smallbizthoughts.com

Email and Web Safety

Extensions that could be dangerous

Programs

- .EXE
- .PIF
- .APPLICATION
- .GADGET
- .MSI
- .MSP
- .COM
- .SCR
- .HTA
- .CPL
- .MSC
- .JAR

Shortcuts / Other

- .SCF
- .LNK
- .INF
- .REG

Office Macros

- .DOC, .XLS, .PPT
- .DOCM, .DOTM, .XLSM, .XLTM, .XLAM, .PPTM, .POTM, .PPAM, .PPSM, .SLDM
- – Newer Office extensions
- - Those that end in X (e.g., .DOCX) contain no macros
- - Those that end in M (e.g., .DOCM) can contain macros

Scripts

- .BAT
- .CMD
- .VB, .VBS
- .VBE
- .JS
- .JSE
- .WS, .WSF
- .WSC, .WSH
- .PS1, .PS1XML, .PS2, .PS2XML, .PSC1, .PSC2
- .MSH, .MSH1, .MSH2, .MSHXML, .MSH1XML, .MSH2XML

Copyright © 2021 Karl W. Palachuk – www.Smallbizthoughts.com

Virus Safety Tips

- You already have an anti-virus program!
  - Don’t “install” another one
  - Don’t click to fix things

- If something pops up – close it
  - Do not click on anything
  - ALT-F4 is better than clicking the “x”

Copyright © 2021 Karl W. Palachuk – www.Smallbizthoughts.com

Social Media – Great for Social Engineering

What kind of bread are you?

- City where you were born
- Mother's maiden name
- Favorite pet
- First car
- What street did you grow up on?

Copyright © 2021 Karl W. Palachuk – www.Smallbizthoughts.com

Newsjacking

- Covid !!!
- Thanksgiving
- Christmas
- Hannukah
- New Years
- Superbowl

- Whatever’s in the headlines

Copyright © 2021 Karl W. Palachuk – www.Smallbizthoughts.com

Recommendations

Copyright © 2021 Karl W. Palachuk – www.Smallbizthoughts.com

Assume You'll Be Attacked

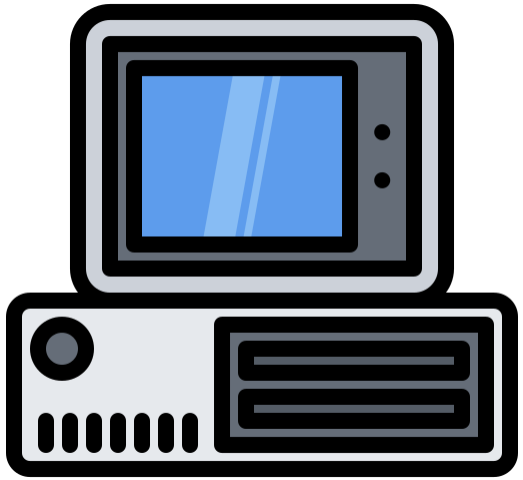
- Large-payoff companies are being targeted
- Everyone else is attacked randomly. Everyone.

- Backups must be tested!
- Be prepared to restore . . . And don't pay the ransom
- Plan your incident response

Copyright © 2021 Karl W. Palachuk – www.Smallbizthoughts.com

Keep Technology Fresh

- Old hardware *cannot* be secured
- Old software can be patched . . . to a point
  - When software is “no longer supported” it cannot be secured
- Apply all patches in a timely manner!
  - Windows, Adobe, Office, Anti-Virus . . . . Everything
  - Reboot at least once a week



Copyright © 2021 Karl W. Palachuk – www.Smallbizthoughts.com

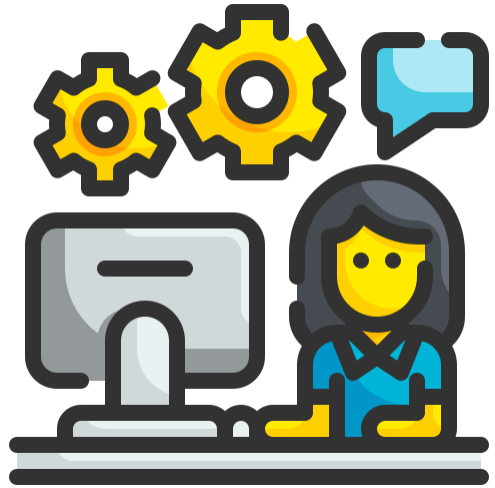
Only Use Company Resources

- NO DropBox
  - (or OneDrive or anything else)
  - No personal cloud storage or email
- No company data on phone unless there's a business reason for it
- Data goes on the official cloud share – NOT the C: drive

Copyright © 2021 Karl W. Palachuk – www.Smallbizthoughts.com

Local Administrator

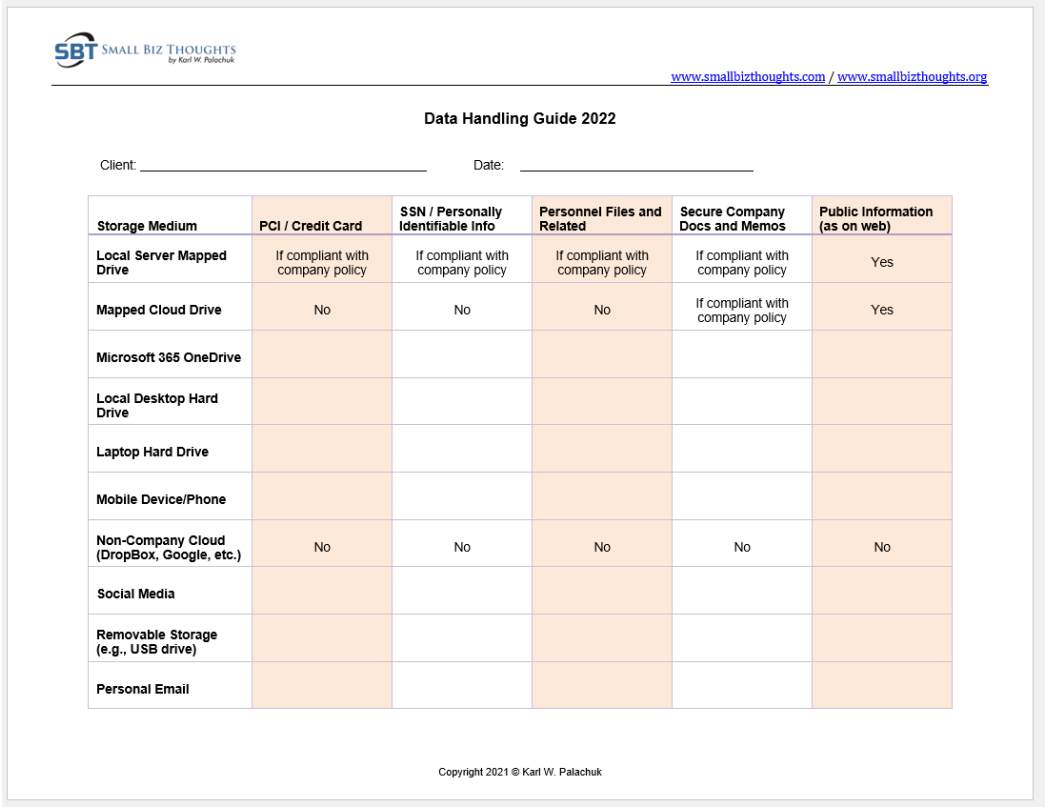
- You are not an administrator on your PC
- Administrator privileges have to be enabled to install software – including viruses
- Your IT Service Provider will install programs for you



Copyright © 2021 Karl W. Palachuk – www.Smallbizthoughts.com

Policies

- Data management
  - Draft “Data Handling Guide”
- Work from home
  - Remote/VPN access
- Acceptable use policy
  - e.g., Email on personal devices
- Backup and data retention policy



SBT Small Biz Thoughts by Karl W. Palachuk

www.smallbizthoughts.com / www.smallbizthoughts.org

Data Handling Guide 2022

Client: _____ Date: _____

Storage Medium	PCI / Credit Card	SSN / Personally Identifiable Info	Personnel Files and Related	Secure Company Docs and Memos	Public Information (as on web)
Local Server Mapped Drive	If compliant with company policy	If compliant with company policy	If compliant with company policy	If compliant with company policy	Yes
Mapped Cloud Drive	No	No	No	If compliant with company policy	Yes
Microsoft 365 OneDrive					
Local Desktop Hard Drive					
Laptop Hard Drive					
Mobile Device/Phone					
Non-Company Cloud (DropBox, Google, etc.)	No	No	No	No	No
Social Media					
Removable Storage (e.g., USB drive)					
Personal Email					

Copyright 2021 © Karl W. Palachuk

Copyright © 2021 Karl W. Palachuk – www.Smallbizthoughts.com

Common Cybersecurity Threats

Malware
Code with malicious intent
Many attacks are a subset of malware

Rogue Software
Malware pretending to be legit

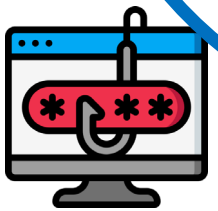
DOS / DDOS
Denial of Service, Distributed DOS

Maladvertising
Infested ads you click on

Password Attacks
Attempt to break in via username/password

Drive-by Downloads
Malware installed on your system

Phishing
Email with evil links



Man in the Middle
Intercept data and impersonate

Copyright © 2021 Karl W. Palachuk – www.Smallbizthoughts.com

Questions . . . Comments

Slides at **bit.ly/sbt-cyber2022**

Karl W. Palachuk

Small Biz Thoughts

karlp@smallbizthoughts.com

Copyright © 2021 Karl W. Palachuk – www.Smallbizthoughts.com