What's on your network?

All About Passwords


SOMEONE FIGURED
OUT MY PASSWORD,
NOW I HAVE TO RENAME MY DOG

Managing Passwords

- Keep your passwords in a secure location
  - Do NOT use paper or sticky notes
  - Do NOT store passwords in clear-text on

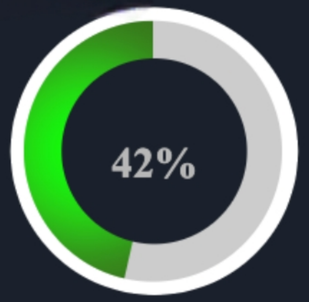
- Utilize a password manager (aka vault)
  - **Bitwarden**
  - KeePass
  - ~~LastPass~~

- Benefits of a password manager
  - One strong password to access them all
  - Passwords are stored securely

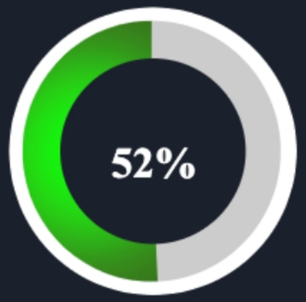
Password Tips

- Avoid using items that can be associated with you
  - Address
  - Phone numbers
  - Pet names
  - Child names
  - Birthdays
  - Sports teams
- Separate passwords for every account
- Auto-generated, near impossible to guess

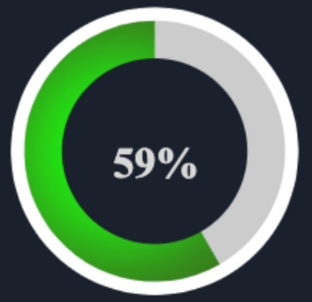
Easy with a password manager



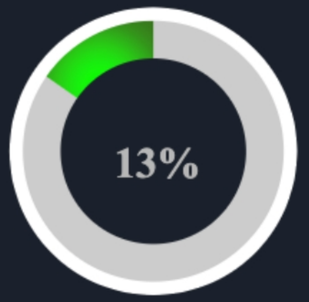
Rely on sticky notes for password mgmt



Re-use password for multiple accounts



Use name or birthdate in password



Reuse same password for all accounts

Source: Comparitech

Activity

Passphrases, not passwords?

- Useful when passwords must be typed in
  - Computer login
  - Wireless <- no phone numbers!
- Should not be easy to guess
  - At least 12 characters, but 15 or more is far better
  - Length better than “complexity” - upper, lower, number, & special characters (~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/)
  - Bad password (8): P@ssw0rd
  - Great password (25): MysonwasbornNovember1995!

Why are most passwords exactly 8 characters?

Top 20 passwords by rank & year

Rank	2020	2021	2022	Rank	2020	2021	2022
1	123456	123456	password	11	1234567	qwerty123	1234567
2	123456789	123456789	123456	12	qwerty	000000	1234
3	picture1	12345	123456789	13	abc123	1q2w3e	1234567890
4	password	qwerty	guest	14	Million2	aa12345678	000000
5	12345678	password	qwerty	15	000000	abc123	555555
6	111111	12345678	12345678	16	1234	password1	666666
7	123123	111111	111111	17	iloveyou	1234	123321
8	12345	123123	12345	18	aaron431	qwertyuiop	654321
9	1234567890	1234567890	col123456	19	password1	123321	7777777
10	senha	1234567	123123	20	qqww1122	password123	123

If you use any of these, change them NOW!!!

Source: Nordpass

Password length <-> time to crack

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	Instant	Instantly	Instantly
7	Instantly	Instantly	2 secs	7 secs	31 secs
8	Instantly	Instantly	2 mins	7 mins	39 mins
9	Instantly	10 secs	1 hour	7 hours	2 days
10	Instantly	4 mins	3 days	3 weeks	5 months
11	Instantly	2 hours	5 months	3 years	34 years
12	2 secs	2 days	24 years	200 years	3k years
13	19 secs	2 months	1k years	12k years	202k years
14	3 mins	4 years	64k years	750k years	16m years
15	32 mins	100 years	3m years	46m years	1bn years
16	5 hours	3k years	173m years	3bn years	92bn years
17	2 days	69k years	9bn years	179bn years	7tn years
18	3 weeks	2m years	467bn years	11tn years	438tn years

Time for an attacker to brute force passwords.

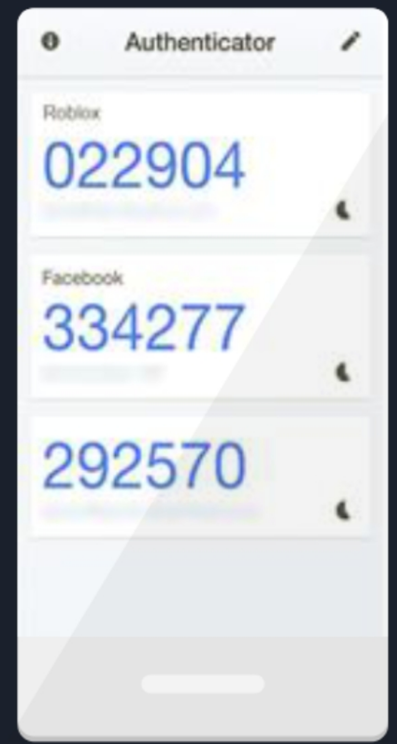
Are you in the yellow or green?

Source: Hive Systems

2FA - two-factor auth

- What is 2FA?
  - "Beyond" a username and password
  - Second form to prove it is you
  - Typically out-of-band
- "Your one-time code is…"
  - SMS
  - Phone call
  - Applications
    - Google Authenticator
    - Microsoft Authenticator
    - Built into password manager?
  - Email
  - Phone pop-up

Not as secure



99.9% LESS likely to be compromised if you use MFA.

Source: Microsoft Tech Community

Password managers & 2FA

Just A Little Click

Is the link safe in 4 steps

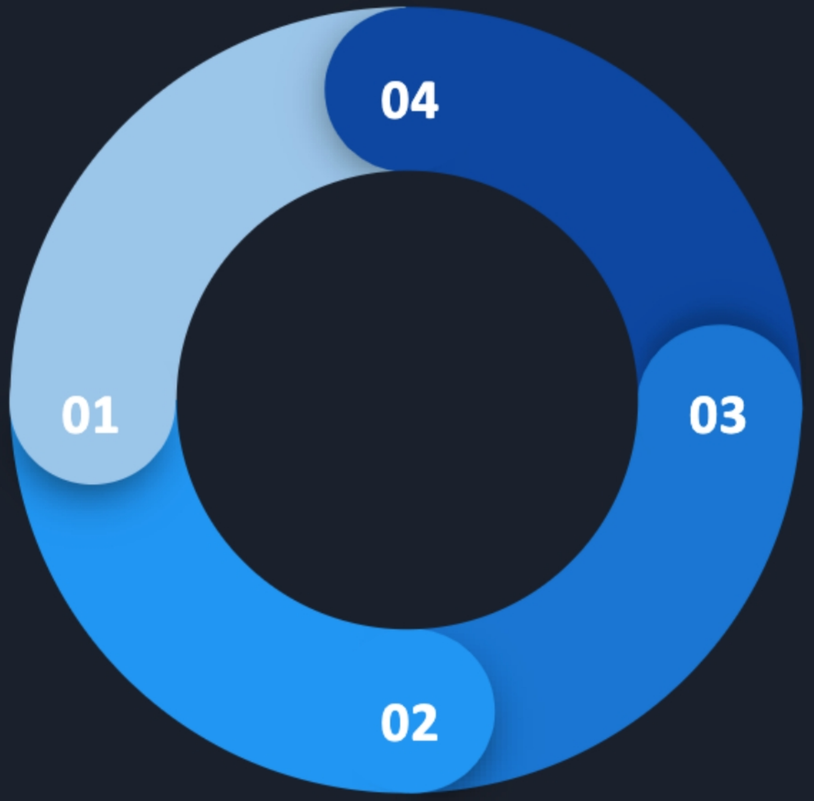
1. Verify

Were you expecting a link?

- Not just email!
- Social Media
- SMS/iMessage
- Zoom, Teams, Slack, etc.

2. Hover

Hover over the link to ensure that it leads to where it says it does



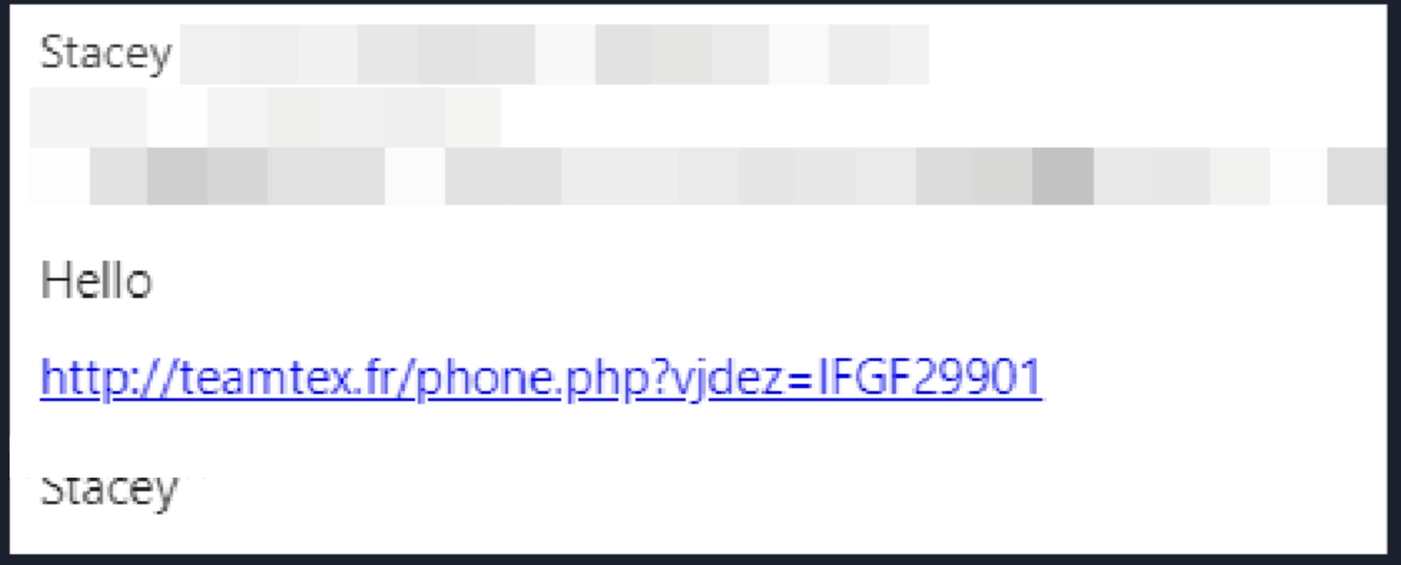
4.CLICK

Does it pass all 3 tests?
Still use caution
“When in doubt, throw it out”

3. Sniff test

Is it a site you recognize?
Does it feel “familiar” to you?
Be skeptical

From known email account



Hacked or spoofed email from someone you know

Similar attacks via Facebook & social media

Red flags?

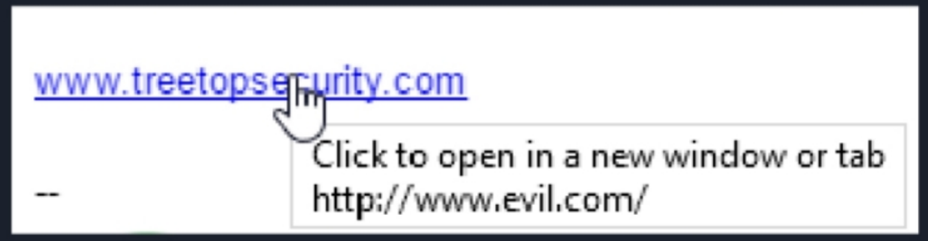
- Email address ok
- Name ok
- Odd “signature”

Expected email?
Link - .fr is France

Hover before you click

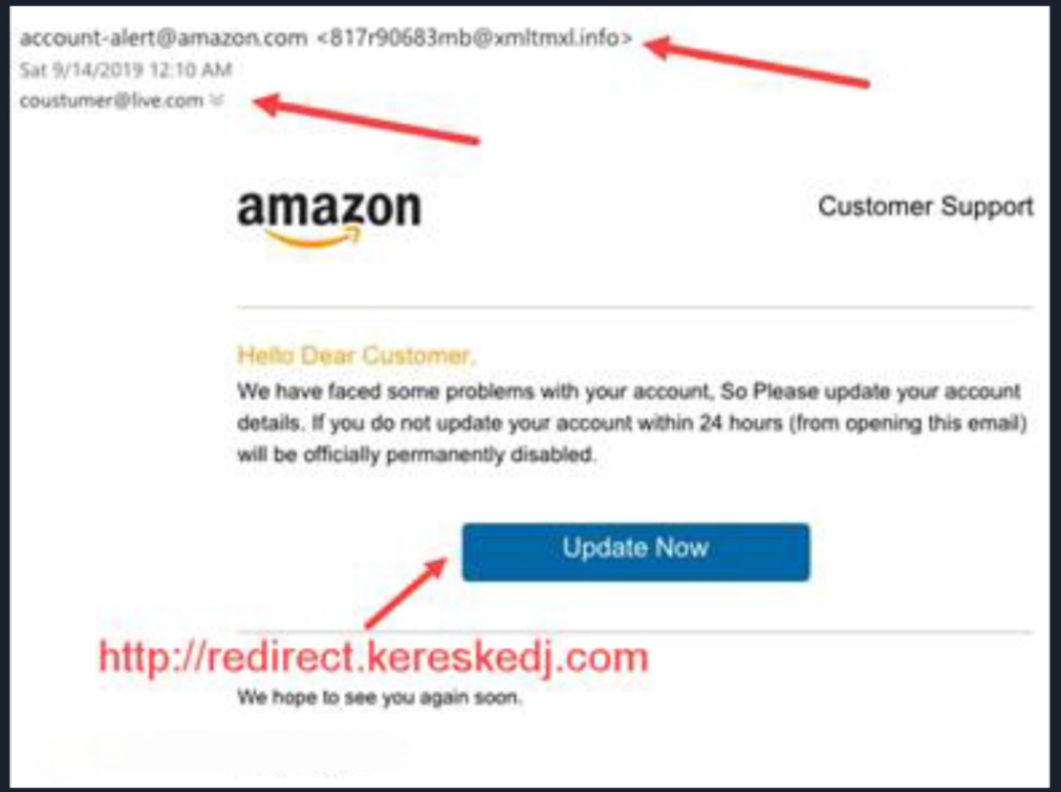
- Why hover?
  - Blue text can be deceiving
  - Underlying URL may be different
  - **"Foregin"** domains - .uk, .cn, or .ru
- Numbers instead of letters
  - Example: 192.168.1.1
  - Don’t trust it!
- Hover on mobile/tablet?
  - Long press (hold)
- Any doubts? Don’t click it!!!

Desktop - Hover



Mobile - Long Press

Hover is your friend



Red flags?

- Email address ok?
- Expected email?
- Sense of urgency
- HOVER!!!

Source: Malware Traffic Analysis

More email attacks

94% of malware is delivered by email

1.2% of all emails sent are malicious

Over three billion phishing emails every day

Sources: ZDNet | Verizon DBIR

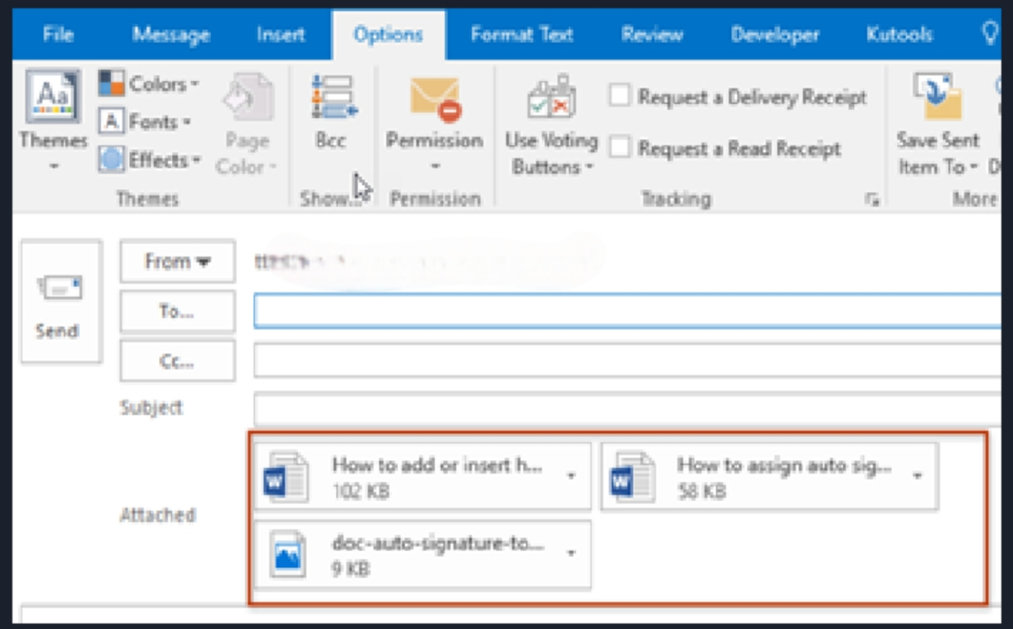
Email Attachments

- Stop & think before you click!
- Recognized sender?
- Expecting attachment?
- Is it normal for that contact to send attachments?

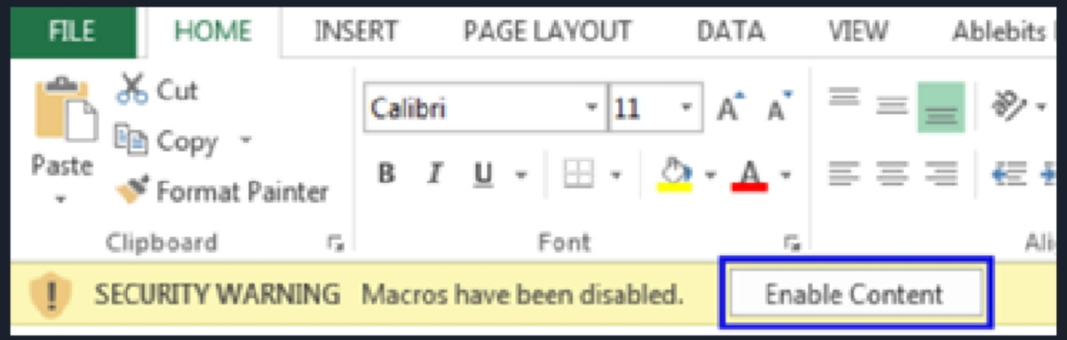
Macros

- Step 1: Don’t do it!!!
- Step 2: See step 1
- Found in downloaded files too

Attachments in email client (Microsoft Outlook)

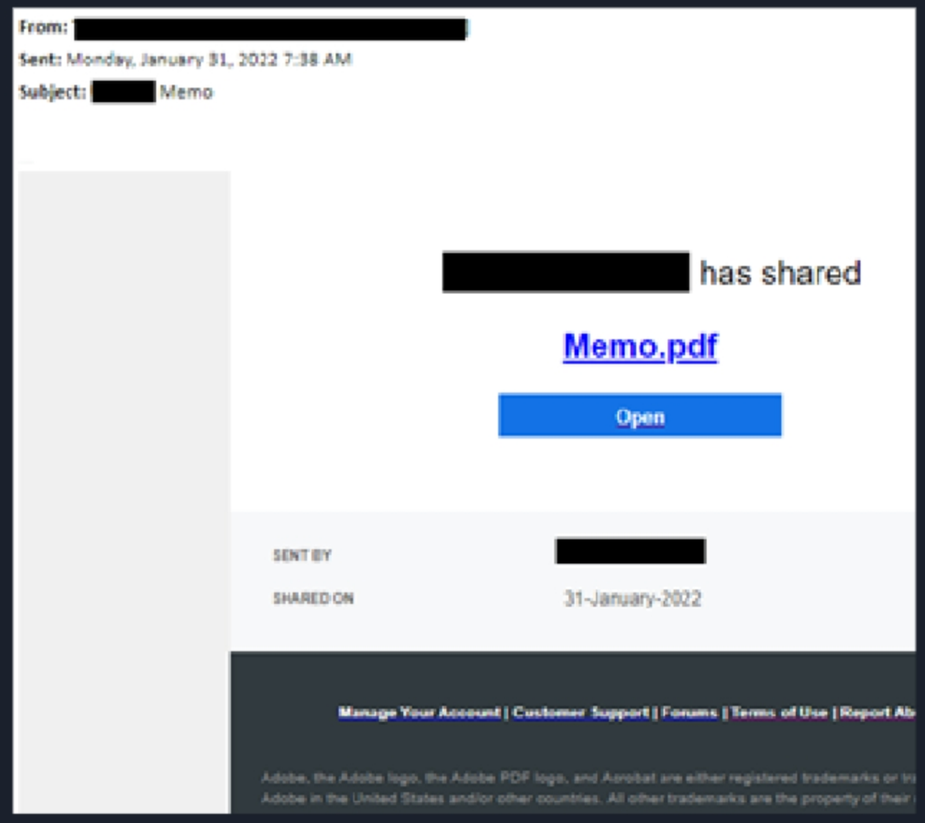


Enable Macros <- NOOOOOO!!!!



Activity

Customer BEC example

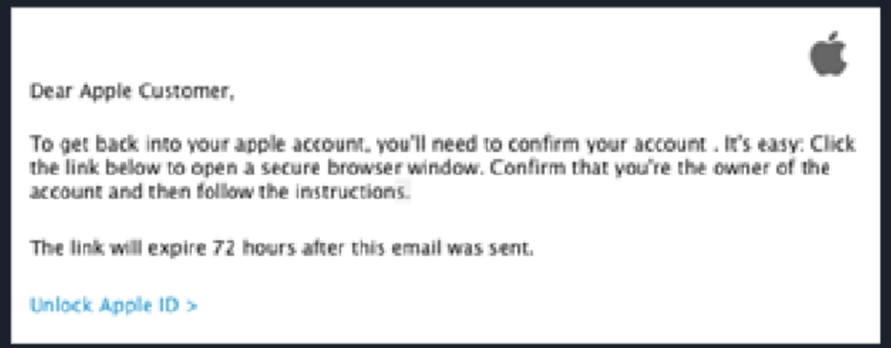


- Small business < 100 employees
- CEO received email
  - From school district (their customer)
  - Bid proposal
  - Busy CEO blocked, certain it was legit
  - Asked us to “bypass” blocks/alerts
- Give us 5 minutes
  - Contacted school IT
  - “You’re the 2nd call”
  - All within 30 mins of 1st alert

Image source: TreeTop Security

Other Email Scams

Account credentials



Dear Apple Customer,

To get back into your apple account, you'll need to confirm your account . It's easy: Click the link below to open a secure browser window. Confirm that you're the owner of the account and then follow the instructions.

The link will expire 72 hours after this email was sent.

Unlock Apple ID >

Technology alone <u>cannot</u> solve this

- Mostly "non-technical"
- What the attackers want
  - Money
    - Gift cards
    - Credit cards
    - Wire transfers
  - Access to email & accounts
- Possible signs
  - Sense of urgency
  - Never happened before
  - No limit on what they say/do

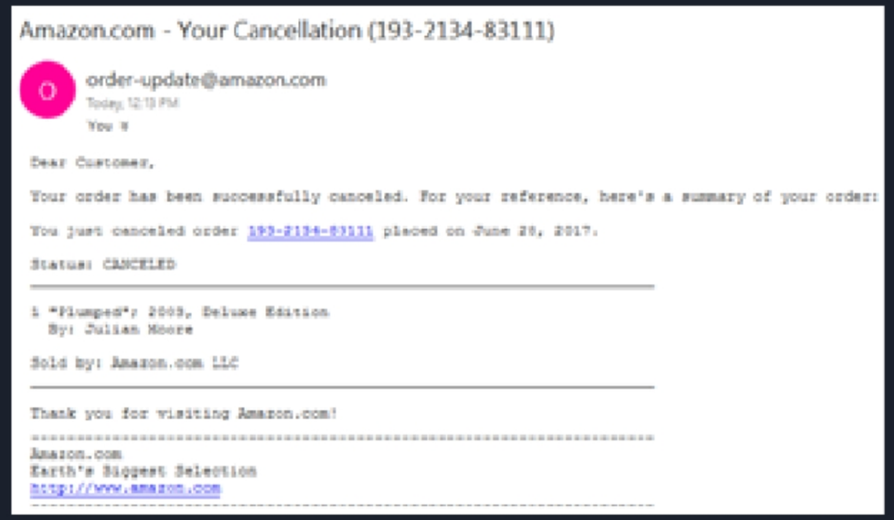
Scammer favorites

- Mimic recent, breaking news
  - Worldwide
    - Health scares
    - Protests
    - Elections
  - Local and regional
- Seasonal/holidays
  - Order & delivery issues
  - Tax issues

Keep your guard up!

Recent events - coronavirus

Order Cancelled




Have you been part
of a breach?

Reach Out & Scam Someone

Activity

Phone Scams

- Social engineering, what is it?
  - Banks & credit card companies
  - Medical & insurance

- Other common **phone scams**
  - Grandparent Scam
  - Tech support - Microsoft, Apple, Dell, etc. will never contact the average user “out of the blue”

Phone scam example

Hi! This is Kathleen from Microsoft. We have been trying to get in touch with you. However, we will be disconnecting your license within 48 hours because your IP address has been compromised from several countries. So we need to change your IP address and license key. So please press 1 to get connected…

Red flags?

- Sense of urgency
- Purposefully confusing
- Expected call from Microsoft?

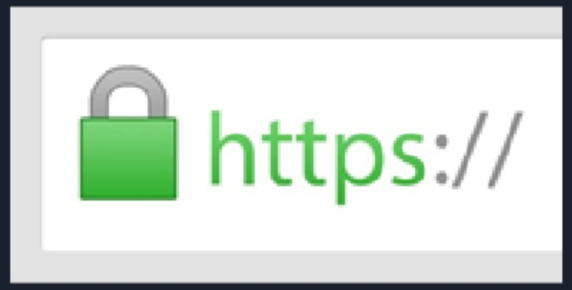
Technical safeguards can only do so much…
That's why security awareness is a must!

General Tips & Privacy

USB Drives & More

- Do NOT connect unknown or unauthorized media (or devices)
- Programs can run when plugged in without you doing anything
- Examples
  - USB/flash drives
  - SD or micro SD cards
  - CDs or DVDs
  - External hard drives
  - Cell phones <- Often forgotten

Encryption



- Can help protect your data
- Can also “help” an attacker, e.g. ransomware
- Protecting data sent or received
  - HTTP❌ vs. HTTPS✓
  - Wireless -> WPA2 (AES) recommended
- Protecting devices
  - Helpful if device is lost/stolen
  - Often associated with phone PIN/passcode
  - Microsoft Windows - BitLocker
  - Apple MacOS - FileVault

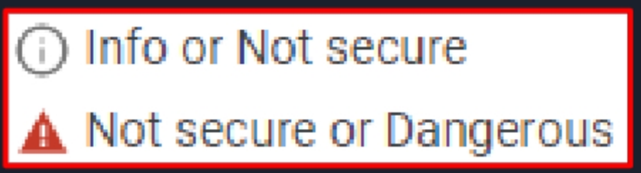
Activity

Internet Safety Quick Tips

- Never click or install anything based on a pop-up from a website
- "Trusted" websites can & have hosted malware, aka malvertising
  - Local news?
  - WSJ, Forbes, ESPN, Yahoo, etc.
  - Limit browsing to business relevant sites?
- Avoid public: Wi-Fi, computers (hotels, libraries), charging, etc.

Do NOT assume a site is legitimate simply because of the "padlock"

No more padlock?



Internet Privacy

- Data is the new gold -> your data is valuable!
- If you're not paying for it, are you the product?
  - Data analytics & predictive results

- Are you oversharing?
  - "Fun" online surveys => data harvesting
  - Default privacy settings on social media

Questions?

by: elbtat