Be Safe Online!

QBE

Cyber criminals are taking advantage of people every day. Don’t worry! You can do things to prevent yourself from being a victim!

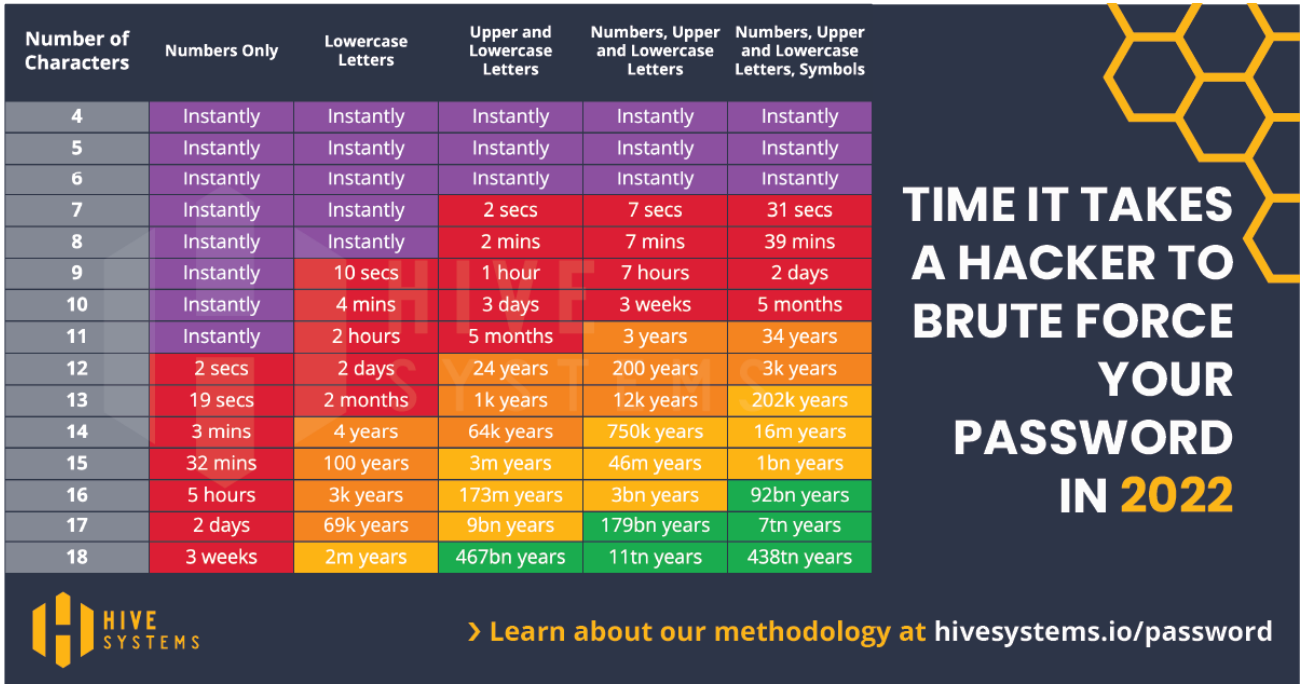
The purpose of this webinar is to give you all practical tips you can use to keep yourself safe online!

Strong and Unique Passwords

- One of the easiest things to keep yourself safe is to use **strong and unique passwords**.
- A strong password will be long and have a combination of letters, numbers, and special characters. **The longer the better!**
- Don’t reuse the same password for multiple logins. They should be unique to each site. **TIP:** Use a good password manager!

- Additional Resources
  - https://www.cisa.gov/sites/default/files/publications/NCSAM_CreatingPasswords_2020.pdf

Strong and Unique Passwords



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	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

According to Verizon, 80% of data breaches are the result of poor or reused passwords!

Image credit: Hive Systems

Multi Factor Authentication (MFA/2FA)

- Use multi/two factor authentication where available.
- This is an extra level of protection in case your password becomes known to others.
- Example of this is a text message with a code that you have to enter to confirm it's actually you.
- Additional Resources:
  - https://www.cisa.gov/MFA

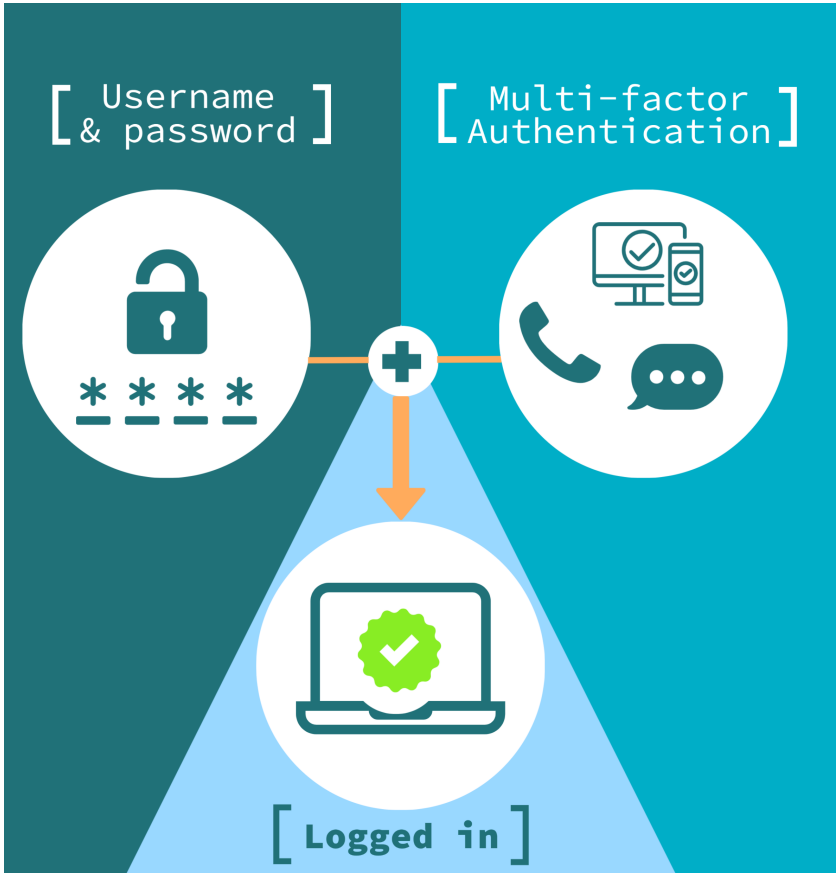


Image credit: https://www.bath.ac.uk/campaigns/layer-up-your-account-security-with-multi-factor-authentication-mfa/

Keep it up to date

- Keep your system and software up to date. Regularly updating your devices and software will fix security holes.
- In addition, it will fix software bugs and even provide new features!
- **TIP:** Restart your devices regularly (phones, tablets, and computers) to ensure updates have been applied.

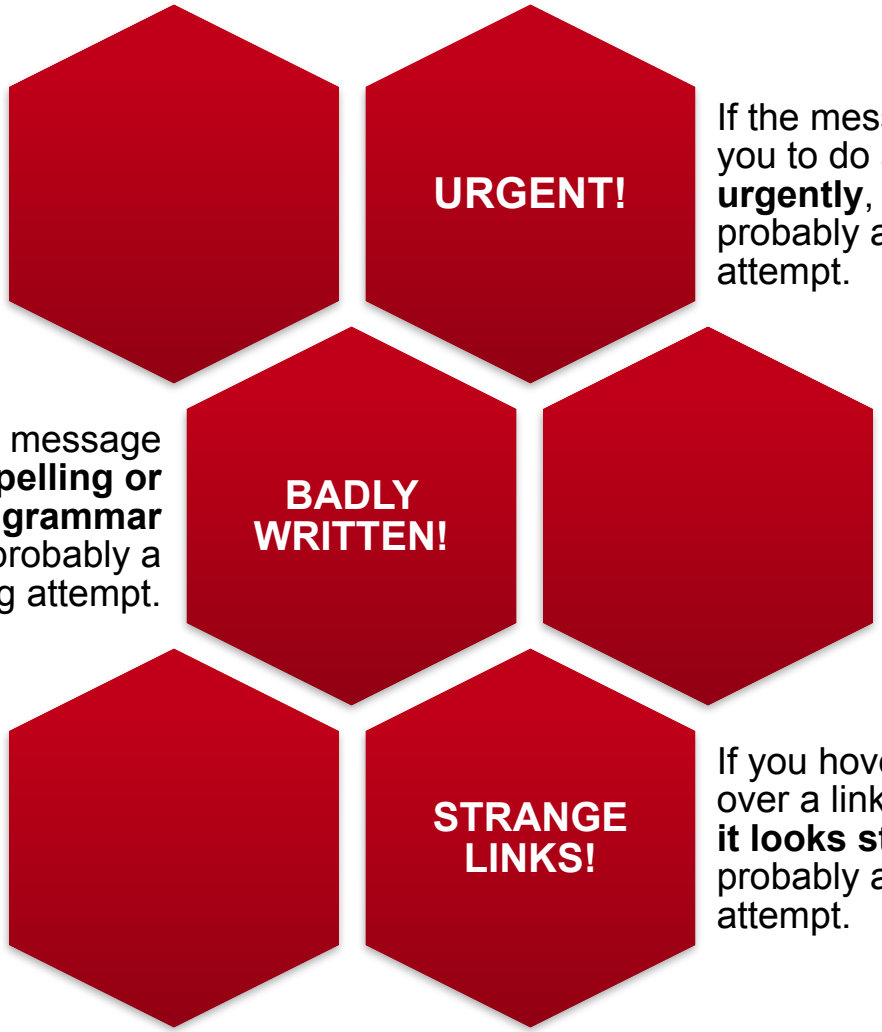
Be careful with email and text messages

- Be on the lookout for suspicious text messages and emails. See examples →
- Don't click on links or open attachments from messages you didn't expect to receive.
- Never give out personal or your confidential information.

1. The IRS is trying to reach you
2. You have a refund
3. You have a package delivery. Please verify
4. You have a new billing statement
5. Congratulations, You won!
6. Verify your bank account details
7. Verify your Apple iCloud ID
8. A family member needs some help
9. Reactivate your account
10. Receive your Bitcoin Gift

Another term for these emails is called **phishing.** When using SMS/ text messages, it's called **smishing.**

What to look out for



If the message asking you to do something **urgently**, then it's probably a phishing attempt.

If the message contains **spelling or other grammar errors**, it's probably a phishing attempt.

If you hover your mouse over a link in email and **it looks strange**, it's probably a phishing attempt.

Spot the Phish!

From: customer_support@bank0famerica.com

To: Marcus Smart

Subject: Take action immediately!

Hello Marcus,

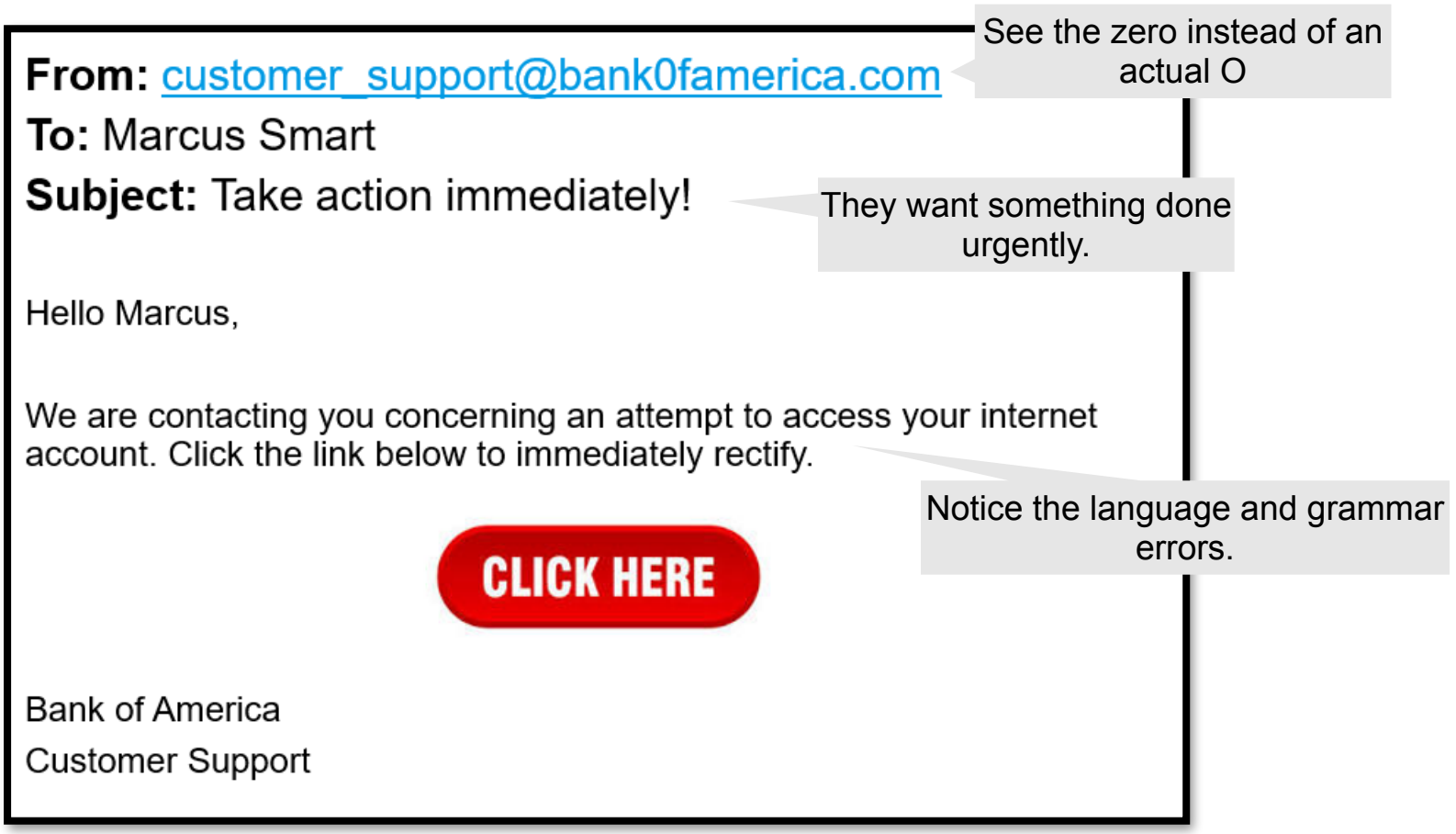
We are contacting you concerning an attempt to access your internet account. Click the link below to immediately rectify.

Bank of America

Customer Support

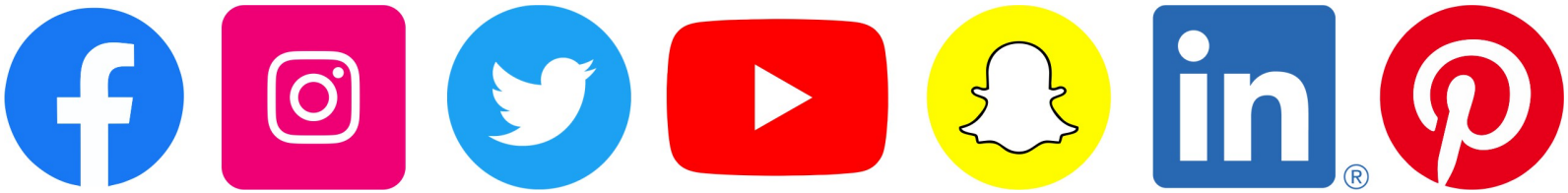
QBE

Spot the Phish!



Social Media Usage

- When using Social Media sites, be conscience of the type of information you post.
- Images being posted should be set to not give out location information.
- Be mindful of public posts asking people to comment with information about yourself (where you grew up, favorite singer, favorite team, etc.)
- Don’t accept friend requests from unknown people even if the user has several friends in common.



BE SAFE OUT THERE!

THANK YOU!