VALLEY STRONG CREDIT UNION

Resources to Protect Your Children, Your Parents and Yourself from On-Line Criminals

For Parents and Caretakers

NetSmartz Workshop

An excellent place for your children to learn how to be safer online.
https://www.netsmartzkids.org/

NSTeens

Helping you make safer choices online. https://www.nsteens.org/

National Center for Missing and Exploited Children

National Center for Missing and Exploited Children is the nation's clearinghouse and comprehensive reporting center for all issues related to the prevention of and recovery from child victimization, NCMEC leads the fight against abduction, abuse, and exploitation - because every child deserves a safe childhood.

https://www.missingkids.org/home
https://www.missingkids.org/education
Tip Line: CyberTipline.com
1-800-The Lost

Scams Calls

Federal Trade Commission (FTC)

Learn about recent scams and how to recognize the warning signs. Read the FTC's most recent alerts or browse scams by topic.
https://www.consumer.ftc.gov/features/scam-alerts

Online Security

Federal Trade Commission (FTC) Online Security

The internet offers access to a world of products and services, entertainment, and information. At the same time, it creates opportunities for scammers, hackers, and identity thieves. Learn how to protect your computer, your information, and your online files.
www.consumer.ftc.gov/topics/online-security

Scammers use email or text messages to trick you into giving them your personal information. But there are several things you can do to protect yourself.
https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams

Do Not Take the Bait
https://www.consumer.ftc.gov/articles/phishing-dont-take-bait

National Cyber Security Alliance (NCSA) Online Safety Basics

Learn how to protect yourself, your family, and devices with these tips and resources.
https://staysafeonline.org/stay-safe-online/

Securing Your Home Network
https://staysafeonline.org/stay-safe-online/securing-key-accounts-devices/securing-home-network/

Protecting Your Identity

***Federal Trade Commission* (FTC) Protecting Your Identity**

While identity theft can happen to anyone, there are some things you can do to reduce your risk.
https://www.consumer.ftc.gov/topics/identity-theft

Ransomware

Here are some tips individuals can take to avoid a ransomware attack. Please visit the FBI, CSA, and FTC sites below to obtain additional information on how to avoid ransomware and what to do if you are a victim of a ransomware attack.

- ✓ *Do not click on emails you do not know who they are from*
- ✓ *Make sure your PC/Laptop operating system, is patched*
- ✓ *Patch your software*
- ✓ *Keep your PC/Laptop clean*
- ✓ *Think before your click*
- ✓ *Ensure anti-virus and anti-malware solutions are set to automatically update and conduct regular scans.*
- ✓ *Back up data regularly and verify the integrity of those backups. Protect your valuable work, music, photos, and other digital information by making an electronic copy and storing it safely. If you have a copy of your data and your device falls victim to ransomware, you will be able to restore the data from a backup.*
    - ❑ *Use Peter Krogh 3-2-1 rule as a guide to backing up your data*
        - ▪ *The rule is: Keep at least three (3) copies of your data, and store two (2) backup copies on different storage media, with one (1) of them located offsite.*
        - ▪ *Secure your backups. Make sure they are not connected to the computers and networks they are backing up. - Veeam Software*

FBI

https://www.fbi.gov/investigate/cyber
Ransomware Overview: https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/ransomware

Cybersecurity and Infrastructure Security Agency CISA

Ransomware Overview: https://www.us-cert.gov/Ransomware

Federal Trade Commission (FTC)

Ransomware Brochure & Quiz: https://www.ftc.gov/tips-advice/business-center/small-businesses/cybersecurity/ransomware

What to Do If You Experience Ransomware

FBI

1. Report the incident to FBI's Internet Crimes Complaint Center https://www.ic3.gov/default.aspx
   - Include any contact information (like the criminals' email address) or payment information (like a Bitcoin wallet number).
2. You can report it to your local FBI Field Office: https://www.fbi.gov/contact-us/field-offices/field-offices

Cybersecurity and Infrastructure Security Agency (CISA)

1. Victims of ransomware should report it immediately to CISA at https://www.us-cert.gov/forms/report or a local FBI Field Office, or Secret Service Field Office.

Secret Service Field Office:

1. **Secret Service Field Office: https://www.secretservice.gov/contact/field-offices/**

How to Report Phishing Scams

If you got a phishing email or text message, report it. The information you give can help fight the scammers.

Step 1. If you got a phishing email, forward it to the Anti-Phishing Working Group at reportphishing@apwg.org.
If you got a phishing text message, forward it to SPAM (7726).

Step 2. Report the phishing attack to the FTC at ftc.gov/complaint.

How to Report Cybercrime

Federal Trade Commission (FTC)

- IdentityTheft.gov to report and recover from identity theft and get a recovery plan and put it into **action.**

FBI: Internet Crime Complaint Center

- FBI Field Office: https://www.fbi.gov/contact-us/field-offices/field-offices
- https://www.ic3.gov/default.aspx

Cybersecurity and Infrastructure Security Agency (CISA)

1. Victims of ransomware should report it immediately to CISA at https://www.us-cert.gov/forms/report , a local FBI Field Office, or Secret Service Field Office.

Other Local Law Enforcement Office

1. **Secret Service Field Office: https://www.secretservice.gov/contact/field-offices/**

Be Smart Be Vigilant on How You Create Your Password By

1. Remember the longer the password; the better so start with using 12 Characters Password length
2. Being unpredictable and creative
   - Includes Numbers, Symbols, Capital Letters, and Lower-Case Letters: Use a mix of different types of characters to make the password harder to crack.
3. A strong passphrase is a random combination of words that are meaningless together.
4. Avoid Bunching Numbers and Symbols Together
   - One good password practice that often goes overlooked it to spread numbers and symbols throughout the password instead of bunching them together, which makes it easier for the password to be hacked.

5. Refrain from Using Dictionary Words
   - Stay away from obvious dictionary words and combinations of dictionary words. Sophisticated hackers have programs that search through tens of thousands of dictionary words.
   - Any word on its own is bad. Any combination of a few words, especially if they're obvious, is also bad. For example, "house12!" is a terrible password. "Redhou1!" is also very bad.
   - Having an 'obvious' password like "Pas$w0r1" makes it easy for hackers to hack: this password is not strong in today's world because hackers have sophisticated ways of cracking a password.

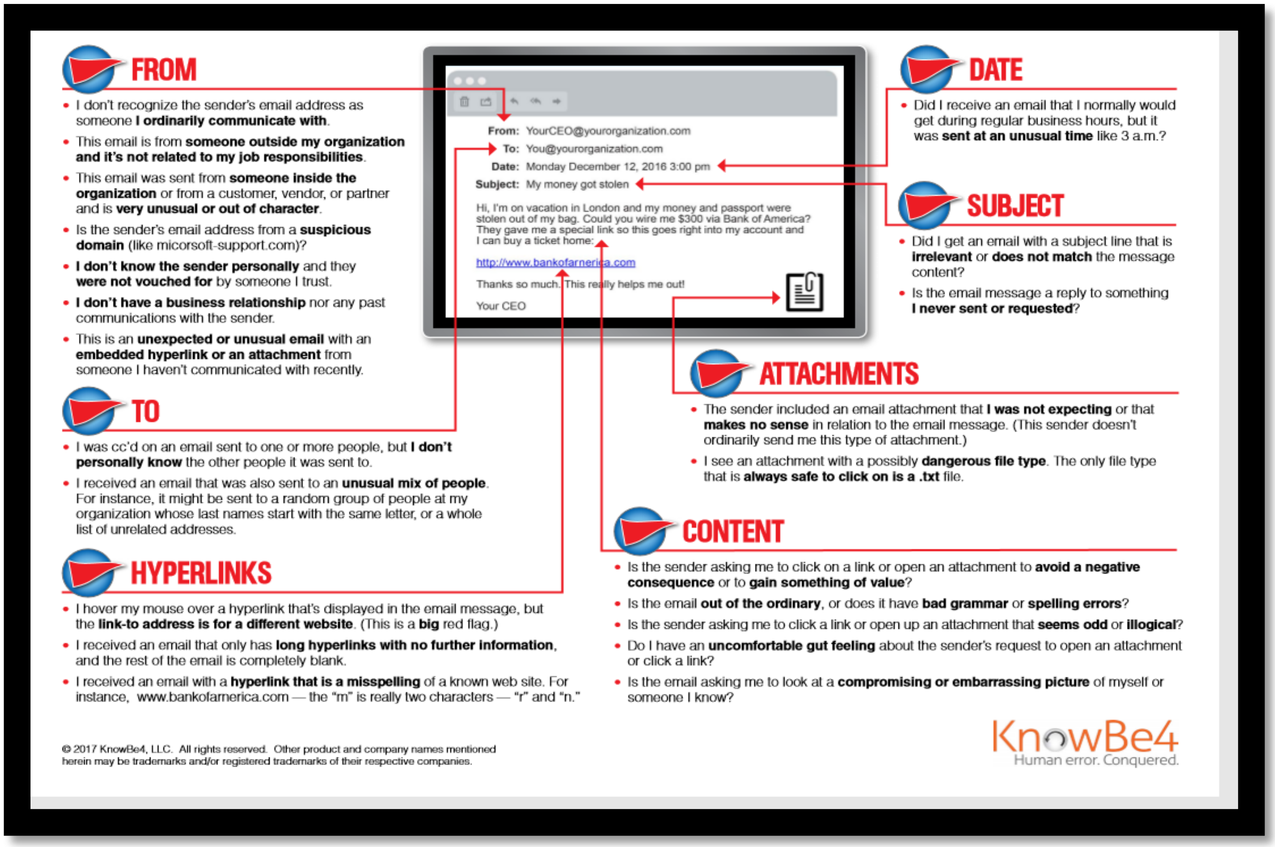
- What makes "Pas$w0r1" a weak password; is it a dictionary word where the first letter is capitalized, the "s" is replaced with $, the number is at the end. B00k123! is another password easy to hack: What makes "B00k123!" a weak password; is it a dictionary word where the first letter is capitalized, the letters "oo" is replaced with zeros "00", the numbers are sequential "123".
- A three-letter sequence that just happened to spell a dictionary word - such as "cat," but the password is Dcatt4674!& works well

6. Please create unique passwords that steer clear of personal information like company names, username, social security number, nickname, date of birth, and a relative's name.

7. Use Different Passwords for Different Accounts
    - It can be tempting to use the same password for every account, so we do not forget our passwords.
      However, this makes it easier for hackers to break into a multitude of accounts. Diversify your passwords by using a different password for every account.

8. Change your password if you think it has been compromised.

Do Not Click on Anything Without First Checking For



From: YourCEO@yourorganization.com
To: You@yourorganization.com
Date: Monday December 12, 2016 3:00 pm
Subject: My money got stolen

Hi, I'm on vacation in London and my money and passport were stolen out of my bag. Could you wire me $300 via Bank of America? They gave me a special link so this goes right into my account and I can buy a ticket home:

http://www.bankofarnerica.com

Thanks so much. This really helps me out!

Your CEO

FROM

- I don't recognize the sender's email address as someone **I ordinarily communicate with**.
- This email is from **someone outside my organization and it's not related to my job responsibilities**.
- This email was sent from **someone inside the organization** or from a customer, vendor, or partner and is **very unusual or out of character**.
- Is the sender's email address from a **suspicious domain** (like micorsoft-support.com)?
- **I don't know the sender personally** and they **were not vouched for** by someone I trust.
- **I don't have a business relationship** nor any past communications with the sender.
- This is an **unexpected or unusual email** with an **embedded hyperlink or an attachment** from someone I haven't communicated with recently.

TO

- I was cc'd on an email sent to one or more people, but **I don't personally know** the other people it was sent to.
- I received an email that was also sent to an **unusual mix of people**. For instance, it might be sent to a random group of people at my organization whose last names start with the same letter, or a whole list of unrelated addresses.

HYPERLINKS

- I hover my mouse over a hyperlink that's displayed in the email message, but the **link-to address is for a different website**. (This is a **big** red flag.)
- I received an email that only has **long hyperlinks with no further information**, and the rest of the email is completely blank.
- I received an email with a **hyperlink that is a misspelling** of a known web site. For instance, www.bankofarnerica.com — the "m" is really two characters — "r" and "n."

DATE

- Did I receive an email that I normally would get during regular business hours, but it was **sent at an unusual time** like 3 a.m.?

SUBJECT

- Did I get an email with a subject line that is **irrelevant** or **does not match** the message content?
- Is the email message a reply to something **I never sent or requested**?

ATTACHMENTS

- The sender included an email attachment that **I was not expecting** or that **makes no sense** in relation to the email message. (This sender doesn't ordinarily send me this type of attachment.)
- I see an attachment with a possibly **dangerous file type**. The only file type that is **always safe to click on is a .txt** file.

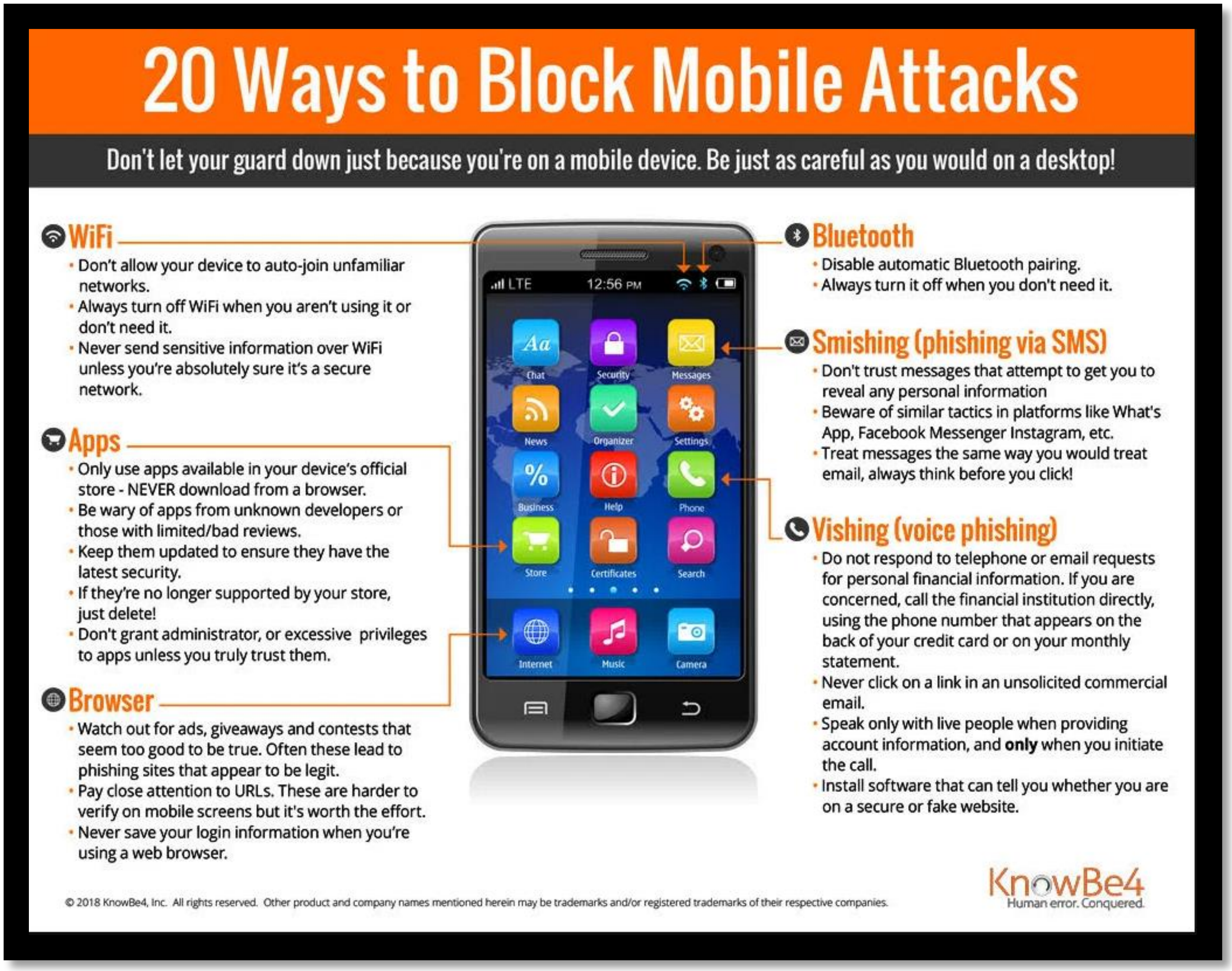
CONTENT

- Is the sender asking me to click on a link or open an attachment to **avoid a negative consequence** or to **gain something of value**?
- Is the email **out of the ordinary**, or does it have **bad grammar** or **spelling errors**?
- Is the sender asking me to click a link or open up an attachment that **seems odd** or **illogical**?
- Do I have an **uncomfortable gut feeling** about the sender's request to open an attachment or click a link?
- Is the email asking me to look at a **compromising or embarrassing picture** of myself or someone I know?

KnowBe4
Human error. Conquered.

Secure Your Mobile Phone

With the growing use of mobile phones to conduct business, shop, and more, mobile devices are becoming a major cause of concern in the security community. Help protect your phone and other mobile devices from hackers by securing your phone with a strong password. Or, better still, use fingerprint or facial recognition passwords to help outwit the hackers.



20 Ways to Block Mobile Attacks

Don't let your guard down just because you're on a mobile device. Be just as careful as you would on a desktop!

WiFi

- Don't allow your device to auto-join unfamiliar networks.
- Always turn off WiFi when you aren't using it or don't need it.
- Never send sensitive information over WiFi unless you're absolutely sure it's a secure network.

Apps

- Only use apps available in your device's official store - NEVER download from a browser.
- Be wary of apps from unknown developers or those with limited/bad reviews.
- Keep them updated to ensure they have the latest security.
- If they're no longer supported by your store, just delete!
- Don't grant administrator, or excessive privileges to apps unless you truly trust them.

Browser

- Watch out for ads, giveaways and contests that seem too good to be true. Often these lead to phishing sites that appear to be legit.
- Pay close attention to URLs. These are harder to verify on mobile screens but it's worth the effort.
- Never save your login information when you're using a web browser.

Bluetooth

- Disable automatic Bluetooth pairing.
- Always turn it off when you don't need it.

Smishing (phishing via SMS)

- Don't trust messages that attempt to get you to reveal any personal information
- Beware of similar tactics in platforms like What's App, Facebook Messenger Instagram, etc.
- Treat messages the same way you would treat email, always think before you click!

Vishing (voice phishing)

- Do not respond to telephone or email requests for personal financial information. If you are concerned, call the financial institution directly, using the phone number that appears on the back of your credit card or on your monthly statement.
- Never click on a link in an unsolicited commercial email.
- Speak only with live people when providing account information, and **only** when you initiate the call.
- Install software that can tell you whether you are on a secure or fake website.

KnowBe4
Human error. Conquered.