# Alva State Bank & Trust Company

# AwesomeSafetyBits

## Social Engineering

Social Engineering is one of the easiest ways that crooks can access your personal information and make money. If you aren't aware of what Social Engineering is, please read this newsletter. This type of crime is based on preying on our emotions. They will target dating sites, social engineering platforms, email and phone. In some cases they request to be your friend and begin to develop some sort of relationship with you- sometimes business, sometimes romantic. Other cases start the converstation very threateningly, claiming to cause harm or defammation if you don't follow their instuctions. Sometimes they promise large sums of money in return for a small role you need to play in purchasing a gift card or wiring money for them. They promise that once you send them 'x' dollars, they will send you thousands more. Some scams involve a crook convincing you to give access to your online banking account information, so they can mobile deposit a check to you. If they actually do mobile deposit a check, the check comes back fraudulent. Some scams send emails containing suspicious links or attachments to a huge number of people just hoping that someone will click.

**RULE OF THUMB.**

If it's too good to be true- it probably is. If you don't know the person contacting you, they probably don't know you either- they are just PHISHING for information. Delete the email or hang up the phone and they will move on to the next (easier) target.

When in doubt. **CALL US!**

## Phishing, explained

Fear is incomplete knowledge

**What is Phishing and why should you care?**

Phishing is a cybercrime where bad guys throw out some bait (email, phone or text message) and see who bites the hook. The criminals lure individuals into providing sensitive data such as account information that is then used to access important accounts and can result in identity theft and financial loss.

http://www.phishing.org

### Common Features of Phishing Emails

1. **Too Good to be True**: Amazing offers and eye-catching or attention grabbing statements are designed to attract people's attention immediately. For example, many claim that you have won a prize.
2. **Sense of Urgency:** **ACT FAST**! Because this super great deal is only for a **LIMITED TIME**! **IGNORE IT.**
3. Hyperlinks: a link within the body of an email may not be all it appears to be. Hover your mouse curser over the links or images in the email and it will highlight the URL that the image or link is going to direct you to. If it is completely different then implied in the context of the email- then **DO NOT CLICK IT**. Often you will notice grammatical errors or misspellings in attempted phishing emails.
4. Attachments: Email attachments you weren't expecting or that doesn't make sense, **DO NOT OPEN THEM**. They often contain things like ransomware, malware or other viruses. The only file type that is safe to click on is a .txt file.
5. **Unusual Sender:** If anything seems out of the ordinary, unexpected, out of character, or suspicious in general, **DON'T CLICK ON IT**. Cyber Criminals can spoof an email to make it look similar to someone from your contact list, making you believe it is safe to open. Other times, someone that you **do** have in your contact list has been hacked themselves, so the email actually **IS** coming from their email, **but they may not know it**. When in doubt, reach out to that contact and verify they sent you the email.

# Alva State Bank & Trust Company

# AwesomeSafetyBits

## Social Engineering Red Flags

### FROM

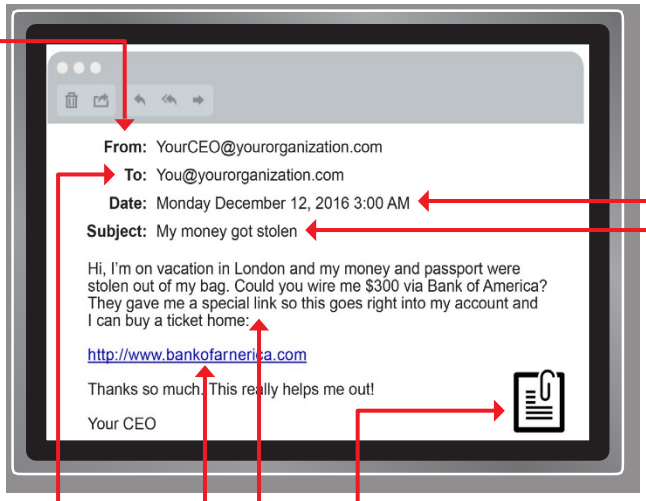
- ✓ Do you recognize the senders email?
- ✓ Does the email address come from a suspicious domain? (like Microsoft-support.com)?
- ✓ Do you know the sender personally? Or has someone you know, vouched for this person?
- ✓ Do you have a business relationship or any past communication with this sender?
- ✓ Does the email have an embedded hyperlink or attachment that you didn't expect?
- ✓ If you don't know the sender, assume it was a mistake or a fraud attempt.

### TO

- ✓ Were you cc'd in the email with people you don't know?
- ✓ Was the email sent to an unusual mix of people?

### HYPERLINKS

- ✓ Hover your mouse over any hyperlink that is displayed in the email message. If the link-to-address is a different website or anything strange, it's probably a scam.
- ✓ Does the body of the email only have hyperlinks that make sense?
- ✓ Does the hyperlink mis-spell any words? Probably a Scam.




### DATE

- ✓ Did you receive an email that you would normally receive during business hours, but it came at a strange time, like 3am?

### SUBJECT

- ✓ Did you get an email with a subject link that is irrelevant or doest not match the message content?
- ✓ Is the email message a reply to something that you never requested?

### ATTACHMENTS

- ✓ Did the sender include an email attachment that you weren't expecting or that makes no sense in relation to the message? Does this sender usually send strange attachments?
- ✓ If the file type of the attachment seems strange? Remember .txt files are the only safe files to click on.
- ✓ When in question, call or text the sender to verify they sent it.

### CONTENT

- ✓ Does the sender ask you to click a link or open an attachment to avoid something negative or to gain something of value?
- ✓ Does the message have bad grammar or spelling?
- ✓ Does the refer to or ask you to view an embarrassing picture?

Stay Alert!

Think BEFORE you Click!

When in doubt CALL US!

Value Your Data

Thank You

## Alva State Bank & Trust Company

*Older than Oklahoma*

**Alva Main Office**
518 College Ave.
Alva, Ok 73717
**580-327-3300**

**Burlington Branch**
PO Box 80
Burlington, Ok 73722
**580-431-3300**

**Enid-Chisholm Branch**
801 W. Broadway
Enid, Ok 73701
**580-234-4201**

**Bank of Freedom Branch**
1085 Main St.
Freedom, Ok 73842
**580-621-3276**

**First State Bank of Kiowa Branch**
546 Main St.
Kiowa, Ks 67070
**620-825-4147**

www.alvastatebank.com 1-800-259-2582 customerservice@alvastatebank.com