PHISHING

DON'T GET HOOKED!

Phishing email messages and websites are intended to steal your money. Cybercriminals can do this by installing malicious software on your computer or stealing personal information off of your computer. They might email you, call you on the phone, or convince you to download something off of a website.

Don't get reeled in! Look for these Phishing scam signs:

- Poor spelling and unusual grammar
- Asking you to type in your password or other confidential information for "security purposes"
- Offering a prize or reward to get you to click on a link
- Website addresses that look almost identical to the real thing but are slightly different:

  www.twiter.com vs. www.twitter.com
- Aggressive urgency to get you to respond in a panic before you even think about it
- Using masked links that look like a familiar website but take you to a different link once you click on it

  Hint: hovering over the link with your cursor will show you the real website address that the link will take you to
- Emails that appear to come from a senior employee from your company or organization

Protect yourself, protect your business. MXOtech will help.

Visit www.mxotech.com/security for more information.

mxotech

Beyond IT. People.

WHAT HAPPENS ON **SOCIAL MEDIA** STAYS ON GOOGLE **FOREVER**

Social media is a wonderful tool for staying in touch with friends and family. But remember, it isn't truly private.

Follow these tips to stay safe:

- If you wouldn't say it in person, don't say it online
- Don't put up any sensitive personal details, such as work or personal information
- Turn on your privacy settings and keep them locked so that only your most trusted friends and family can see what you post
- Log out of the application every time you’re done using it (this way if you lose your phone, your accounts can’t be easily accessed)
- Use a different password for all of your social media accounts

mxotech
Beyond IT. People.

Protect yourself, protect your business. MXOtech will help.

Visit www.mxotech.com/security for more information.

PASSWORDS
ARE LIKE UNDERPANTS

✗ You shouldn't leave them out where people can see them
✓ You should change them regularly
✗ And you shouldn't loan them out to strangers

Here are tips to creating a strong password:

GOOD PASSWORDS

- ✓ Are at least 14 characters in length
- ✓ Are a phrase, instead of a single word: “iLOveMYp4sswOrd!”
- ✓ Contains both upper and lower case letters and some punctuation
- ✓ Are not single words in any language, slang or dialect
- ✓ Do not include personal information such as names of family, pets, etc.

BAD PASSWORDS

- ✗ Can be found in a dictionary in any language
- ✗ Contain less than 10 characters
- ✗ Are easy to figure out like family, pets, birthdays, etc.
- ✗ Use word or number patterns

mxotech
Beyond IT. People.

Protect yourself, protect your business. MXOtech will help.

Visit www.mxotech.com/security for more information.