EMAIL SECURITY
BEST PRACTICES

In 2019, the number of email phishing scams and ransomware infections more than doubled from previous years. Now more than ever, it's important to take steps to protect yourself and your organization's security. Here's a quick top ten list for keeping the online bad guys out of your inbox.

1 Don't trust a sender's information like names or positions.

Hackers know how to make their emails look like they come from a senior employee within your own organization. Be sure to look at the email address to confirm the true sender.

2 Look, but don't click.

Use your mouse to hover over the link with your cursor. This shows you the real website address of the link before you click on it. If the link looks strange or doesn't match what the link description says, don't click on it.

3 Check for spelling errors.

Spelling and grammatical errors are an immediate red flag that the link may be harmful.

4 Beware when asked to provide personal information.

Phishing emails will often ask for passwords or other confidential information for "security purposes."

5 Make passwords looonger.

When it comes to password security it's the length of the password that matters, not the frequency they are changed. Use 3 or 4 words together to make your password at least 21 characters long.

6 Beware of urgency.

Phishing emails are frequently threatening or aggressive in nature. The hackers hope you will respond out of panic and a sense of urgency.

7 Use password best practices.

Use different passwords for each account and don't make them obvious, like birthdays or a family member's name. Don't keep your passwords written on a post-it under your keyboard!

8 Use caution with attachments.

If you see any attachment you are not expecting from a source you don't recognize, verify the sender before opening it. Hackers use enticing tricks like naming attachments "invoice," "RFP," and other legitimate sounding names.

9 Carefully check website addresses.

Phony website addresses look almost identical to the real thing but are slightly different. Examples are:
www.faceb00k.com vs. www.facebook.com
www.twiter.com vs. www.twitter.com
amazon.warehouse.com vs www.amazon.com.

10 Don't believe everything you see.

If something seems slightly off, it's better to be safe than sorry. Make sure to report it to your IT department for verification.

ICONIC IT
better together

www.IconicIT.com

REFERRAL PROGRAM
ICONIC IT better together

TWO WAYS TO EARN

Free Month Of Service

$500 cash

Learn More at: **go.iconicit.com/Referral**

100% MONEY BACK • ICONIC PROMISE