SECURITY AWARENESS NEWSLETTER

DO NOT GIVE YOUR PASSWORD OVER THE PHONE TO ANYONE CLAIMING TO BE FROM THE HELPDESK OR TECH SUPPORT

No one from the HelpDesk or Tech Support will ever ask you for your password. If we need to access your account for some reason, and cannot contact you in time, we will reset the password and notify you by voicemail. Anyone calling and asking you for your password is most likely trying to gain unauthorized access to our network. If you receive such a call, notify your supervisor immediately.

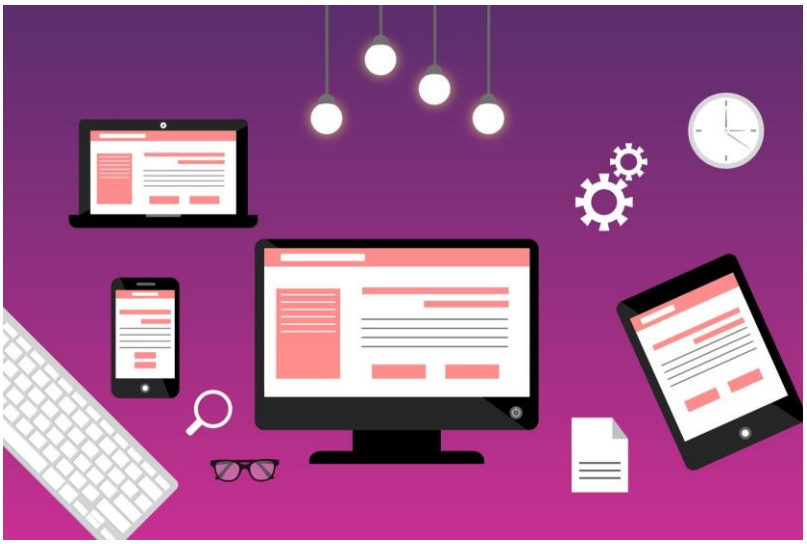
OUTSMART HOAX E-MAIL

Productivity-sapping e-mail circulates close to April Fool's Day. Keep the e-mail system from bogging down with thousands of unnecessary messages—delete hoaxes and jokes.

One year, an April Fool e-mail claimed that "for every person that you forward this e-mail to, Microsoft will pay you $245.00 ..." It was forwarded to thousands of people even though it sounded too good to be true. At one nationwide company, in-boxes were clogged and the e-mail servers had to be reset, delaying legitimate e-mail.

CYBER ZONES
Cyber Security Services

SECURITY AWARENESS NEWSLETTER



How to spot a phishing email...

It could be a phishing email if...

There are misspelled words in the e-mail or it contains poor grammar.

The message is asking for personally identifiable information, such as credit card numbers, account numbers, passwords, PINs or Social Security Numbers.

There are "threats" or alarming statements that create a sense of urgency. For example: "Your account will be locked until we hear from you" or "We have noticed activity on your account from a foreign IP address."

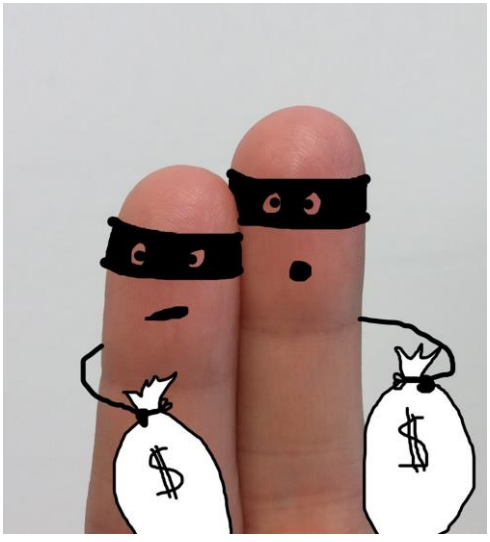
The domain name in the message isn't the one you're used to seeing. It's usually close to the real domain name but not exact. For example:

o Phishing website: www.regionsbanking.com

o Real website: www.regions.com

Think twice before you post personal information. Remember, even crooks may see what you post on social media sites

Criminals are mopping up because social media users are willing to share personal information about themselves and others. This data can be used to guess your password, give them the answers to account security questions or send you email with malicious attachments that appear to be from someone you know.



Use a password protected screen saver

Desktop computers should be locked, or logged off when the user steps away from the terminal.

Password protecting the Windows screen saver is "locking" the desktop. To do this, right click on the desktop and go to "Properties"; select the "Screen Saver" tab; and check "On resume, password protect".