Computer Basics & Reminders

Ask me about getting these set up.

☐ Sign up for Secure Backup Service: visit rowleyservices.com for a free trial & setup info.

☐ Consider occasional full backups. If you want local backups (to an external drive) or occasional full backups, let me know.

☐ Secure main accounts using two-factor authentication (2FA). Hackers do far more damage than people realize until it happens to them. It's easier and smarter to protect your accounts now so that you don't regret it later.
Ask me about Account Security. ☐ Email, ☐ Apple, ☐ Google, ☐ MSFT, ☐ Amazon, ☐ Facebook, ☐ Yahoo, ☐ Comcast
☐ BackBlaze (Online Backup), ☐ Banks, ☐ ALL Transaction Notifications, ☐ Investment Accounts, ☐ PayPal, ☐ eBay

☐ Freeze your credit – Ask for the template with directions and to keep track of the 6 different accounts PER PERSON. Understand that your personal info has already been stolen by identity thieves multiple times, it is only a matter of time before they will use YOUR info. Credit monitoring is NOT the same as freezing your credit.

☐ Turn on EVERY transaction alert / text message notification for EVERY Credit Card, Debit Card, Checking Account, Savings Account, Investment Account, etc. Set the notification limit to $1 so you are notified of EVERY transaction. Enable both text AND email notification for abnormal transactions such as Wires, out of country charges, ATM withdrawal's, etc.

☐ Call right away if you get a virus. Stop using your computer. Hackers use viruses to steal your logins, bank, and CC info.

☐ Keep ALL of your data on your computer, and not on external drives or USB / thumb drives, CD's, etc. Do not trust cloud service providers as your main and/or only location for your photos and data.

☐ Ask me about getting your pictures from your phone to your computer. Don't rely on Apple or Google as a backup.

☐ Unsubscribe from unwanted emails to reduce the amount of junk you have to delete. This can also help reduce the amount of spam and phishing emails that try to trick you into giving up your account credentials. Do not open emails in your junk or spam folders. Unsubscribe from about 20 - 30 per day.

☐ Take Pictures of any Error Messages.

☐ Keep track of all your usernames and passwords ACCURATELY in your password book.

☐ When signing into your various websites, use Chrome Bookmarks and use your saved usernames and passwords.

☐ DO NOT USE YOUR PHONE NUMBER as your USERNAME for sites like Google, Microsoft, or Amazon, etc.

☐ Call me BEFORE purchasing a new Phone or Computer. I will help you find the best deal.

_____ I will NOT "google" or search for phone numbers for customer service.
_____ I will NOT allow strangers or scammers to remote control my computer.
_____ I will NOT fall for calls or fake emails from Microsoft, Amazon, Norton, etc.
_____ I will NOT SHARE account Info, passwords, or security codes over the phone.
_____ I understand that VPN's are a form of PRIVACY and will NOT secure my accounts.
_____ I understand that if a friend asks me to buy a gift card, it IS a scammer, and not my friend.
_____ I understand that bitcoins and gift cards are often used by scammers to steal money.
_____ I understand that if I change my cell phone number I will be permanently locked out of some accounts.
_____ I will not withdraw cash if directed by a scammer that is acting as someone from my bank.
_____ I understand that searching increases virus'. I will use BOOKMARKS and the ADDRESS BAR CORRECTLY.
_____ I will use Chrome and the built-in Chrome Password Manager, so I don't type my passwords into fake sites.

Phishing Emails & Scams

Remember: NEVER BUY GIFT CARDS or Bitcoins

☐ I have read and understand.

Name: _____

Date: _____

Oops! It looks like you got tricked by a scam or phishing email.

It is important to understand that there is no ONE way to tell if an email is legitimate, however, there are many ways to know if the email is a phishing attempt or scam.

There are several ways to tell if an email is a phishing attempt or scam:

1. **Check the email sender's EMAIL ADDRESS (not just the name):**
    a. Check the EMAIL address of the SENDER. IT IS A SCAM if it's from a random email address (@hotmail.com, @gmail.com, @outlook.com, etc.).
    b. Just because an email address LOOKS legitimate, does not mean that the email is from that sender or safe.
    c. So, if an email address looks correct, DO NOT TRUST IT, it still could be a scam.

2. **Check the content of the email:**
    a. Emails threatening to close your account.
    b. Emails urging you to sign in or verify your account.
    c. Emails urging you to update or change your password that is about to expire.
    d. Emails about shipments or packages.
    e. Emails about getting a refund for a service or product.
    f. Emails that have "attachments" that are actually just links to another site.
    g. Emails threatening that you will be charged or that you were already charged.
    h. Emails with links to follow. It is generally advised to NOT click ANY links in emails.
    i. Emails requesting you to confirm your account details to UNLOCK your account.
    j. Emails urging you to "take action" before a certain date or time (usually within 24-48 hours).
    k. Emails from Microsoft, Google / Gmail, Norton, McAfee, etc. are most commonly sent by scammers.

3. **Do you even have "that" service or product?**
    a. Many people are tricked into opening email and following links for services that they don't even have. People who get scammed often say: *"I got an email from McAfee about a bill / charge, but I don't have McAfee. So, I opened the email to make sure they didn't have my credit card info and that they weren't going to charge me".* DO NOT FALL FOR THIS. This is exactly how the scammers want you to respond.

4. **Links in emails:**
    a. Most phishing and scam emails have phone numbers to call or links to click (some just want you to reply via email to them).
    b. On the computer you can use your mouse to HOVER OVER THE LINK then the **FULL and ACTUAL** link address will appear (usually in the bottom left-hand corner of the screen).
    c. If the link address looks fake (ex: microsoft-email.com/sign-in/) then you know the email is a scam.

Remember: Use this info to know that the email is a scam (none of this will tell you that the email is legitimate or safe).

There are tons of new types of phishing and scam emails that are being created. It is usually better to be cautious and assume that it's a scam first, then ask for help if you are not 100% certain.

None of the large companies like Microsoft will ever "lock you out of your account", or "charge you" if you don't follow the email directions within 24-48 hours. NONE OF THEM USE TIME LIMITS LIKE THAT.

If you have an email that you really think is legitimate, but you are still unsure, just CALL ME.

Derek Rowley – (253) 564-7777 – Computer Repair & Tutoring – Printed: 20 Aug 2024