|  |  |  |
| --- | --- | --- |
| Slide 1 |  | I want to give a quick update on two scams – one that is new and on the rise. |
| Slide 2 |  | This is a scam that the US Secret Service reports is seeing a sharp increase in recently. Criminals are posing as property owners and through a series of impersonations are negotiating the sale of properties which are vacant or lien free. Often times the “seller” is looking to sell the property fast, below market value. Sometimes there is an explanation, such as a medical emergency or family emergency.  The criminal usually says they have a preference for a cash buyer, and will want to conduct all communications via email/text and will want to have a remote closing.  Ways to prevent this:   * Research the owner of the property * Request an in person or face-to-face meeting (video call) with the seller * Be alert when a seller wants a cash offer below market value for a fast sale – this isn’t always nefarious, but it should raise red flags * Use trusted title companies and attorneys for closings |
| Slide 3 |  | Known as “Business email compromise” or “BEC” or “Email Account Compromise” or “EAC”, a criminal sends an email message that appears to come from a known source making a legitimate request seeking to obtain something from you – whether money or information.  The scammer might:   * Spoof an email account or website. In this case, the scammer makes a slight variation on legitimate addresses by adding/removing a letter or changing “.com” to “.org” * Send “spear phishing emails” where they trick victims into revealing confidential information. This information is then used to access company accounts, calendars, and data that they use to continue to seem legitimate. They may seek information from you that they will then use against someone else. * Use malware which allows the scammer access to the company network. They then use this access to time requests or send messages to make things, like invoices, look more legitimate.   Ways to protect against these scams:   * Change your email passwords often * Use complex passwords and do not repeat passwords for different accounts. * Use a password manager and/or two factor authentication * Don’t click on links in unsolicited emails or texts. If you receive a message asking you to verify or update your account information, go directly to the website of the company that is supposedly requesting the information or update. * Carefully examine email addresses, URLs, and spelling used in all communications. * Be especially wary if you are being pressed to act quickly. |