

Дистанционные мошенничества

Преступления в сфере it-технологий

1. Звонки сотрудников банка и полиции

Сотрудники банка не звонят своим клиентам.

Сотрудники Центрального банка не обслуживают физических лиц.

Сотрудники полиции и ФСБ не привлекают к сотрудничеству гражданских лиц в ходе телефонного разговора.

Сотрудники банков и правоохранительных органов никогда не попросят Вас произвести манипуляции с банковскими счетами и денежными средствами.



2. Торговые площадки «Авито» и «Юла»

Мошенник может выступать как в роли продавца, так и покупателя.

Общение по поводу покупки/продажи необходимо осуществлять только на торговых площадках.

Ни в коем случае не переходить по ссылкам, представленным «покупателем».



3. Родственник попал в беду (ДТП, совершил преступление)

Чаще всего, жертвами мошенников становятся пожилые граждане.

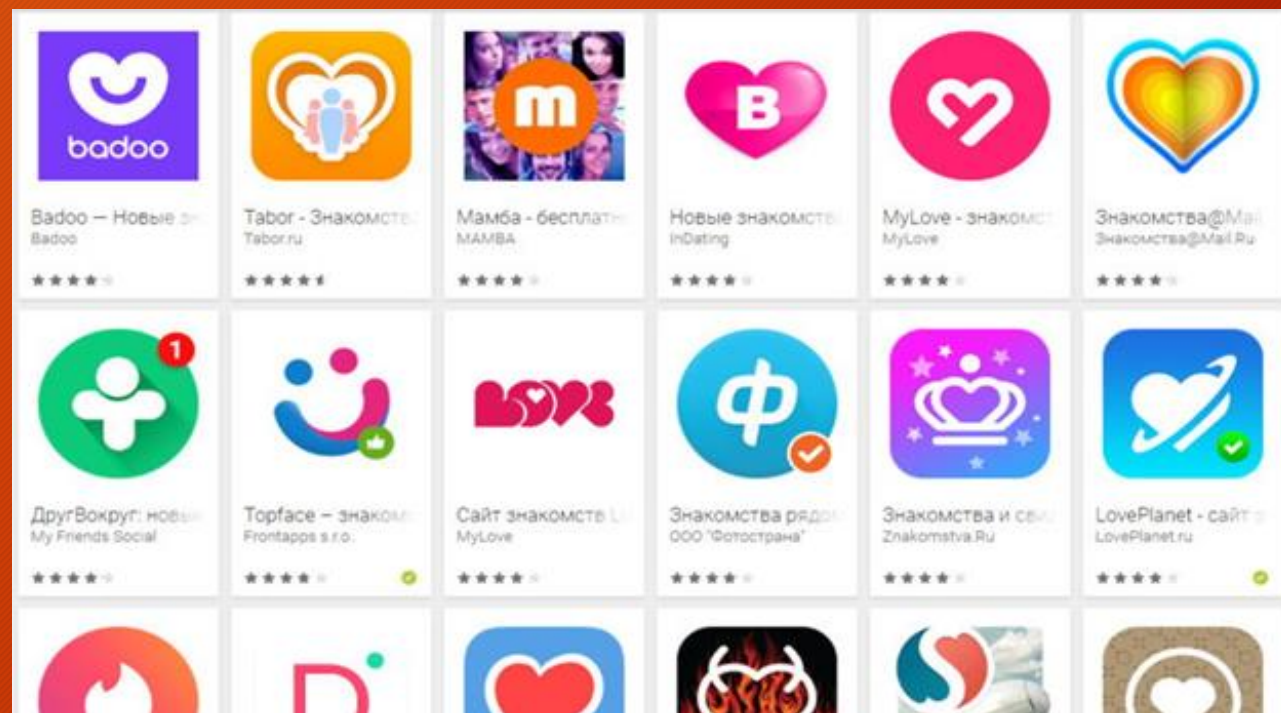
К потерпевшим приезжает курьер, который забирает денежные средства.



4. Сайты знакомств

Обратить внимание, где в дальнейшем девушка/парень предлагает продолжить общение (мессенджеры).

Не переходить по ссылкам с целью приобретения билетов в кино, театр, на стендап.



5. Фишинговые сайты

Всегда проверять наименование ip.
Пробовать зайти на данный сайт
через другие браузеры.

The image shows a browser window displaying a phishing website. The address bar shows the URL myetherwallet.com.im, which is underlined in red. The website header features the MyEtherWallet logo and navigation links. The main content area is titled "Send Ether & Tokens" and asks "How would you like to access your wallet?" with radio button options: Keystore File (UTC / JSON), Private Key, Mnemonic Phrase, Ledger Nano S, and TREZOR. A note indicates "Parity Phrase: No longer supported".

Overlaid on the right side of the browser window is a Slack message from @slackbot. The message text is: "@bancor_bot asked me to remind you 'Please be advised that we are experiencing some errors in the Bancor tokens network. Please visit Myetherwallet to check your tokens balance and update your contract. Failure to do so may result in loss of Bancor tokens. Thank you for your cooperation and understanding.'" A red arrow points from the message to the phishing website's header.

Below the Slack message, there is a red text box with the following text: "Ссылка якобы на кошелек MyEtherWallet от якобы настоящего саппорта в слэке ICO Bancor. Обращение ко всем членам слэка приходит на почту каждому участнику. Пример очень удачного фишинга :)"

At the bottom of the browser window, the address bar shows "Secure https://www.myetherwallet.com" with three exclamation marks (!!!) to its right. A red underline is drawn under the entire address bar area.

Фишинговый сайт!

Правильный адрес:

Secure https://www.myetherwallet.com !!!

6. Инвестиции

Не инвестировать денежные средства на иностранных платформах.

Криптовалюта не признана денежной единицей в РФ.



Сайты-помощники

Phonenum.info

Zip.ru

Finanso.com