[illegible]

[illegible]

[illegible]¡
[illegible]

[illegible]

[illegible]

[illegible] (Consistent) [illegible].
• [illegible] (Immutable) [illegible].
• [illegible] (Ownable) [illegible].
• [illegible] (Canonical) [illegible] (Decentralized) [illegible].

[illegible] (Single Point Failure) [illegible].

[illegible]

[illegible] (Layer 2) [illegible].

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible] IT [illegible] 70 [illegible]

Новый способ защиты от кражи денег со счетов банка через сайты

Банк России предупреждает о новом способе кражи денег со счетов банка через сайты. Он основан на том, что мошенники создают сайты, которые выглядят как официальные сайты банка. Они используют похожие названия и дизайн, чтобы обмануть клиентов. Когда клиент вводит свои данные на таком сайте, мошенники получают доступ к его счету и могут украсть деньги. Банк России рекомендует клиентам быть внимательными и проверять адрес сайта перед вводом данных. Также банк предупреждает о том, что мошенники могут использовать фишинговые письма, которые содержат ссылки на такие сайты. Клиентам не следует переходить по ссылкам из подозрительных писем. Банк России также рекомендует использовать двухфакторную аутентификацию для защиты своих счетов.

Новый способ

Мошенники создают сайты, которые выглядят как официальные сайты банка

[Банк России предупреждает о новом способе кражи денег со счетов банка через сайты](#)

Как это

Мошенники используют различные способы, чтобы заставить клиентов перейти на такие сайты. Они могут отправлять фишинговые письма, которые содержат ссылки на такие сайты. Они также могут использовать рекламу в интернете, чтобы привлечь клиентов. Когда клиент переходит на такой сайт, мошенники получают доступ к его счету и могут украсть деньги. Банк России рекомендует клиентам быть внимательными и проверять адрес сайта перед вводом данных. Также банк предупреждает о том, что мошенники могут использовать фишинговые письма, которые содержат ссылки на такие сайты. Клиентам не следует переходить по ссылкам из подозрительных писем. Банк России также рекомендует использовать двухфакторную аутентификацию для защиты своих счетов.

Банк России также рекомендует клиентам использовать антивирусное программное обеспечение для защиты своих компьютеров от вредоносных программ. Мошенники могут использовать вредоносные программы, чтобы получить доступ к данным клиентов. Банк России также рекомендует клиентам использовать надежные пароли для защиты своих счетов. Пароли должны быть сложными и содержать буквы, цифры и специальные символы. Банк России также рекомендует клиентам не использовать один и тот же пароль для нескольких счетов. Если мошенники получат доступ к одному счету, они могут получить доступ и к другим счетам.

Банк России также рекомендует клиентам быть внимательными при использовании банкоматов. Мошенники могут установить на банкоматы специальные устройства, которые позволяют им получить доступ к данным клиентов. Банк России также рекомендует клиентам использовать банкоматы, которые находятся в безопасных местах. Банк России также рекомендует клиентам не использовать банкоматы, которые выглядят подозрительно. Если клиент заметил что-то подозрительное, он должен немедленно сообщить об этом в банк.

Банк России также рекомендует клиентам быть внимательными при использовании интернет-банкинга. Мошенники могут использовать фишинговые письма, которые содержат ссылки на такие сайты. Банк России также рекомендует клиентам использовать надежные пароли для защиты своих счетов. Пароли должны быть сложными и содержать буквы, цифры и специальные символы. Банк России также рекомендует клиентам не использовать один и тот же пароль для нескольких счетов. Если мошенники получат доступ к одному счету, они могут получить доступ и к другим счетам.

Банк России также рекомендует клиентам использовать двухфакторную аутентификацию для защиты своих счетов. Двухфакторная аутентификация требует от клиента ввести не только пароль, но и код, который отправляется на его мобильный телефон. Банк России также рекомендует клиентам не использовать общедоступные компьютеры для доступа к своим счетам. Банк России также рекомендует клиентам не использовать общедоступные сети Wi-Fi для доступа к своим счетам. Банк России также рекомендует клиентам не использовать общедоступные компьютеры для доступа к своим счетам.

Банк России также рекомендует клиентам быть внимательными при использовании мобильных приложений. Мошенники могут использовать вредоносные программы, чтобы получить доступ к данным клиентов. Банк России также рекомендует клиентам использовать надежные пароли для защиты своих счетов. Пароли должны быть сложными и содержать буквы, цифры и специальные символы. Банк России также рекомендует клиентам не использовать один и тот же пароль для нескольких счетов. Если мошенники получат доступ к одному счету, они могут получить доступ и к другим счетам.

Банк России также рекомендует клиентам использовать двухфакторную аутентификацию для защиты своих счетов. Двухфакторная аутентификация требует от клиента ввести не только пароль, но и код, который отправляется на его мобильный телефон. Банк России также рекомендует клиентам не использовать общедоступные компьютеры для доступа к своим счетам. Банк России также рекомендует клиентам не использовать общедоступные сети Wi-Fi для доступа к своим счетам. Банк России также рекомендует клиентам не использовать общедоступные компьютеры для доступа к своим счетам.

Банк России также рекомендует клиентам быть внимательными при использовании социальных сетей. Мошенники могут использовать социальные сети, чтобы получить доступ к данным клиентов. Банк России также рекомендует клиентам использовать надежные пароли для защиты своих счетов. Пароли должны быть сложными и содержать буквы, цифры и специальные символы. Банк России также рекомендует клиентам не использовать один и тот же пароль для нескольких счетов. Если мошенники получат доступ к одному счету, они могут получить доступ и к другим счетам.

Банк России также рекомендует клиентам использовать двухфакторную аутентификацию для защиты своих счетов. Двухфакторная аутентификация требует от клиента ввести не только пароль, но и код, который отправляется на его мобильный телефон. Банк России также рекомендует клиентам не использовать общедоступные компьютеры для доступа к своим счетам. Банк России также рекомендует клиентам не использовать общедоступные сети Wi-Fi для доступа к своим счетам. Банк России также рекомендует клиентам не использовать общедоступные компьютеры для доступа к своим счетам.

Банк России также рекомендует клиентам быть внимательными при использовании электронной почты. Мошенники могут использовать фишинговые письма, которые содержат ссылки на такие сайты. Банк России также рекомендует клиентам использовать надежные пароли для защиты своих счетов. Пароли должны быть сложными и содержать буквы, цифры и специальные символы. Банк России также рекомендует клиентам не использовать один и тот же пароль для нескольких счетов. Если мошенники получат доступ к одному счету, они могут получить доступ и к другим счетам.

Банк России также рекомендует клиентам использовать двухфакторную аутентификацию для защиты своих счетов. Двухфакторная аутентификация требует от клиента ввести не только пароль, но и код, который отправляется на его мобильный телефон. Банк России также рекомендует клиентам не использовать общедоступные компьютеры для доступа к своим счетам. Банк России также рекомендует клиентам не использовать общедоступные сети Wi-Fi для доступа к своим счетам. Банк России также рекомендует клиентам не использовать общедоступные компьютеры для доступа к своим счетам.

□□□□□□ □□□□□ □□ □ □□□□□ □□□□□□□□□ □ □□□□□□□□ □□□□□ □□□□□□□□□□ □□□□□□□□□□ □□ □□□□□ □□□ □□□□□□ □□□□□ □□□□□
□□□□□□ □□□□□ □□ □□ □□□□□□□□□□ □ □□□□□□□□□□□□ □□□□□□ □□□□□ .□□ □□□□□□ □□□□□ □□□□□ □□ □□□ □□□□□ □□□□□□ □□□□□□□
□□□□□□□□ □□ □□□□□□□□ □□□□□□□ □□□□□ □□ □□□□□□ □□□□□ □□□□□ □□□□□□□ □□□□□□□ □□□□□□□□ □□ □□□□□□□□ □□□□□□□:
□□ □□ □□□□□ □□□□ .□□□□□□ □□□□□□ □□□□ □□ □□□□□□□□ □□□□□ □□□□ □□□□□ □□□□□ □□□□□ □□□□□□ □□□□□□□ □□□□□□□□ □□□□□□□□»
□□□□□□□ □□□ □□ □□□□□ □□□□ □□□□□□ □□□ □□□□ □ □□ □□□□□□ □□□□ □□□□□□□□ □□ □□□□ □□□□ □□□□□□ □□ □□□□□ □□□ □□□□□□□ □□□□□□.»
□□□□□□□□:
□□□□□□□ □□□□□□
□□□□ □□□□:
□□□□□ □□□□□□□
□□□□□□ □□□□□□□:
08:30 - 26/12/1397
□□□□□:
□□□□□□□ □□□□□□ - □□□□□ □□□□□□□ □□□□□□□ - □□□□□□ □□□□□□□ □□□□ □□□□□□ - □□□□ □□□□□

□□□□□
□□□□:https://www.shabakeh-mag.com/cover-story/14813/%D8%B2%D9%86%D8%AC%DB%8C%D8%B1%D9%87-%D8%A8%D9%84%D9%88%DA%A9%DB%8C-%DA%86%DB%8C%D8%B3%D8%AA-%D9%88-%DA%86%D8%B1%D8%A7-%D9%BE%DB%8C%D8%A7%D8%AF%D9%87%E2%80%8C%D8%B3%D8%A7%D8%B2%DB%8C-%D8%A2%D9%86-%D9%81%D8%B1%D8%A2%DB%8C%D9%86%D8%AF%DB%8C-%D9%BE%DB%8C%DA%86%DB%8C%D8%AF%D9%87-%D9%88-%D8%AF%D8%B4%D9%88%D8%A7%D8%B1-%D8%A7%D8%B3%D8%AA%D8%9F