University of Massachusetts
Amherst • Boston • Dartmouth • Lowell • Medical • Law • Online

University of Massachusetts
Tips for Safe Zelle® Payments

- **Update your security settings**
  - Change your security settings to enable multifactor authentication.

- **Protect yourself from phishing calls and emails**
  - Fraudsters/scammers use sophisticated email & phone techniques to gain access to your information. They will spoof calls and send emails that look like they are from your bank. **Beware of clicking links in emails or text messages. Never provide any information over the phone if contacted by someone stating they're from your bank. Hang up and call your bank at the phone number listed on the back of your bank-issued debit card or on the bank's official website**.

- **Don't share personal details online**
  - Avoid sharing your location, home address, phone number and other personal information across social media. Check your settings and permissions on each social platform, and activate any additional security features available, like two-factor authentication. Also, don't accept friend/connection requests from people you don't know.

- **Use strong passwords**
  - Don't use the same password for every site. Don't share your passwords with anyone.

- **Beware on public Wi-Fi**
  - Using free public Wi-Fi may save you some gigabytes on your data plan, but it can come with risks. If you choose to log onto a free Wi-Fi guest network, make sure you don't log onto any secure sites, such as your mobile or online banking sites.

- **Additional Resources**
  - **Articles:**
    1. Helpful Tips for Using Mobile Payments Services and Avoiding Risky Mistakes
    2. Tips on Using Peer-to-Peer Payment Systems and Apps

  - **Websites:**
    1. Consumer Information | Federal Trade Commission (ftc.gov)
    2. Consumer Financial Protection Bureau (consumerfinance.gov)